jamk.fi

Always On VPN -etäyhteysratkaisun toteuttaminen

Atte Manninen

Opinnäytetyö
Toukokuu 2020
Tekniikan ala
Insinööri (AMK), Tieto- ja viestintätekniikka

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Manninen, Atte	Opinnäytetyö, AMK	Toukokuu 2020
	Sivumäärä 72	Julkaisun kieli Suomi
		Verkkojulkaisulupa myönnetty: x

Työn nimi
Always On VPN -etäyhteysratkaisun toteuttaminen

Tutkinto-ohjelma
Insinööri (AMK), Tieto- ja viestintätekniikka

Työn ohjaaja(t)
Jarkko Puistovirta, Jarmo Nevala

Toimeksiantaja(t)
Yritys X

Tiivistelmä

Opinnäytetyön toimeksiantona oli toteuttaa toimiva VPN-etäyhteysratkaisu testiympäristöön, jonka avulla voidaan kartoittaa ratkaisun toimivuutta sekä vertailla sitä nykyiseen tuotannossa olevaan etäyhteysratkaisuun. Tavoitteena oli toteuttaa samankaltainen etäyhteysratkaisu kuin tuotannossa oleva, joka mahdollistaa mahdollisimman helpon käyttökokemuksen loppukäyttäjälle. Testiympäristön avulla suunnitteleminen ja asioiden testaus voidaan toteuttaa turvallisesti sekä myöhemmin ottaa testiympäristön ratkaisu käyttöön myös tuotantoympäristössä.

Etäyhteysratkaisun testiympäristö ja sen testaaminen toteutettiin työpaikan tiloissa. Testiympäristö sisälsi fyysisen palvelimen lisäksi virtuaalipalvelimia sekä verkkolaitteita. Ympäristö toteutettiin mukaillen yrityksen nykyistä tuotantoympäristöä, jolloin vertailu kahden eri etäyhteysratkaisun välillä on helpompaa. Testauksessa käytettiin Windows 10 -työasemaa, jolla testattiin etäyhteyttä ja etäyhteysprofiilin automatisointia.

Tutkimusmenetelmänä käytettiin kehittämistutkimusta, jonka tuloksina saatiin toteutettua vertailua kahden etäyhteysratkaisun välillä, sekä vastauksia käyttöönottoon liittyvissä asioissa. Selvitettäviä asioita tuotantoon asti viemiselle jäi vielä, mutta tarvittavat pohjatiedot hankittiin, joiden avulla varsinaista tuotantoon viemistä voidaan lähteä suunnittelemaan tarkemmin.

Lopputuloksena saatiin toteutettua toimiva testiympäristö, sekä tietoa uudesta etäyhteysratkaisusta. Testiympäristöä ja hankittua tietoa voidaan hyödyntää tuotantoympäristön ratkaisun suunnittelussa ja käyttöönotossa.

Avainsanat (asiasanat)
Always On VPN, etäyhteys

Muut tiedot (Salassa pidettävät liitteet)

jamk.fi

Description

Author(s)	Type of publication	Date
Manninen, Atte	Bachelor's thesis	May 2020
		Language of publication: Finnish
	Number of pages: 72	Permission for web publication: x

Title of publication

Implementation of Always On VPN remote access solution

Degree programme

Information and Communications Technology

Supervisor(s)

Puistovirta Jarkko, Nevala Jarmo

Assigned by

Company X

Abstract

The assignment of the bachelor's thesis was to implement a working VPN remote access solution in a test environment and compare it to an existing remote access solution. The solution had to have the same functionality as the existing remote access solution that provides the easiest possible way to end users to use remote access. The new VPN remote access solution is to be implemented in the production environment later.

Test environment for remote access solution and its final testing were implemented at workplace premises. The environment consisted of virtual servers implemented to one physical server. The firewall and network switches were also used in the test environment. For easier comparison of both remote access solutions, the test environment needed to be built similar like the production environment. The new remote access solution was finally tested on a Windows 10 laptop which was used to test the connectivity of remote access and automation of remote access profiles.

Development research was used as the research method. The answers to the research questions provided information on the two remote connectivity solutions and to the deployment related issues. There are still matters which need to be clarified before implementing the solution to the production environment. However, necessary basic information was acquired which is important part of the planning of the implementation to the production environment.

The final result was a functional test environment as well as information about the new remote access connection solution. The test environment and acquired information can be used to planning and implementation of the production environment solution.

Keywords/tags (subjects)

Always On VPN, remote access

Miscellaneous (Confidential information)

Sisältö

Kuviot

Taulukot

Lyhenteet

AD	Active Directory
AD CS	Active Directory Certificate Services
AD DS	Active Directory Domain Services
AH	Authentication Header
CA	Certificate Authority
CHAP	Challenge-Handshake Authentication Protocol
DC	Domain Controller
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EAP	Extensible Authentication Protocol
EKU	Enhanced Key Usage
ESP	Encapsulated Security Payload
FQDN	Fully Qualified Domain Name
GPO	Group Policy Object
GRE	Generic Routing Encapsulation
HTTPS	Hypertext Transfer Protocol Secure
IIS	Internet Information Services
IKEv2	Internet Key Exchange version 2
IP	Internet Protocol
IPSec	Internet Protocol Security
ISATAP	Intra Site Automatic Tunnel Addressing Protocol
KSP	Key Storage Provider
L2TP	Layer 2 Tunneling Protocol
MDM	Mobile Device Management
NLS	Network Location Server
NPS	Network Policy Server
OU	Organizational Unit
PAP	Password Authentication Protocol
PEAP	Protected Extensible Authentication Protocol
PKI	Public Key Infrastructure
PPP	Point-to-Point Protocol

PPTP	Point-to-Point Tunneling Protocol
RADIUS	Remote Authentication Dial In User Service
RAS	Remote Access Server
RRAS	Routing and Remote Access Service
SA	Security Association
SCCM	System Center Configuration Manager
SSL	Secure Sockets Layer
SSTP	Secure Socket Tunneling Protocol
TLS	Transport Layer Security
TPM	Trusted Platform Module
TTLS	Tunneled Transport Layer Security
UDP	User Datagram Protocol
VLAN	Virtual LAN
VPN	Virtual Private Network
WAN	Wide Area Network
WIP	Windows Information Protection
XML	Extensible Markup Language

1 Johdanto

Hyvin usean yrityksen työntekijöille on tarpeellista päästä työpaikan verkkoon myös työpaikan ulkopuolelta ja tähän tarpeeseen on olemassa erilaisia etäyhteysratkaisuja. Etäyhteysratkaisut ovat kehittyneet paljon vuosien saatossa ja niiden käyttöönotto on samalla lisääntynyt paljon. Tärkeimpiä asioita etäyhteyksien kannalta nykyisin ovat yhteyden turvallisuus ja sen käytettävyys. Uusimpien etäyhteysratkaisujen tavoitteena onkin mahdollistaa käyttäjille mahdollisimman yksinkertainen ja huomaamaton käyttökokemus, turvallisuutta unohtamatta.

Toimeksiantona oli toteuttaa Always On VPN -etäyhteysratkaisu testiympäristöön, jonka avulla toimeksiantajalle saadaan tarvittavaa tietoa uudesta tekniikasta ja sen käyttöönottoon liittyvistä asioista. Lähtökohtaisesti uuden ratkaisun vieminen tuontantoympäristöön ei ole vielä ajankohtaista, joten tarkoituksena on tarjota valmiudet tuotantoympäristön ratkaisun suunnittelulle ja erilaisten asioiden testaamiselle. Varsinainen päämäärä on varautua muutokseen ja hankkia tietoa valmiiksi etukäteen, jotta siirtymävaihe etäyhteysratkaisusta toiseen toteutuu tulevaisuudessa mahdollisimman helposti. Työn avulla jokaisella toimeksiantajan järjetelmänvalvojalla on mahdollisuus perehtyä uuden etäyhteysratkaisun tietoperustaan ja käyttöönottoon. Tämä mahdollistaa sen, että jokainen asiaankuuluva henkilö on tietoinen tekniikasta tai pystyy saamaan tarvittaessa tietoa aiheesta helposti. Näin minimoidaan riski, että kaikki tieto uudesta aiheesta on vain yhden henkilön tietona, joka voi aiheuttaa ongelmia esimerkiksi henkilön irtisanoutuessa.

Työssä tutustutaan VPN-tekniikoihin, kahteen etäyhteysratkaisuun, Windows-palvelimiin, sekä palvelinympäristön tarjoamiin ominaisuuksiin, joilla työn varsinaisen aiheen eli Always On VPN -etäyhteysratkaisun toiminta voidaan toteuttaa. Työ sisältää myös testiympäristön rakentamisen sekä Always On VPN -etäyhteysratkaisun käyttöönoton.

2 Tutkimusasetelma

Opinnäytetyön tarkoituksena oli tutkia ja verrata kahta eri etäyhteysratkaisua sekä saada vastauksia niihin liittyviin tutkimuskysymyksiin. Tutkimuskysymykset koskevat uutta Always On VPN -ratkaisua, sekä käytössä olevaa Direct Access -ratkaisua ja ne ovat seuraavat:

1. Mitä toimivaan Always On VPN -etäyhteysympäristöön tarvitaan?
2. Kuinka Always On VPN -etäyhteysympäristö pystytetään?
3. Miten Always On VPN eroaa nykyisestä Direct Access -etäyhteysratkaisusta?

Keskeisimpiä asioita näissä kysymyksissä on informatiivisen tiedon kerääminen molemmista ratkaisuista sekä vertailu kahden ratkaisun välillä. Vastauksia kysymyksiin etsittiin toteutetusta testiympäristöstä, käytössä olevasta tuotantoympäristöstä, teoriapohjaisista lähteistä ja Yritys X:n asiantuntijalta.

Tutkimusmenetelmänä käytettiin kehittämistutkimusta, sillä selkeänä päämääränä oli mahdollinen muutos yrityksen infrastruktuurissa. Kehittämistutkimuksessa kehittäminen ja tutkiminen yhdistyvät muodostaen prosessin, joka sisältää teoreettisia ja kokeellisia vaiheita. Kehittämisen tulisi pohjautua teoriaan ja tämän lisäksi tuottaa uutta teoriaa. Lähestymistapoja kehittämistutkimukselle on useita ja sillä on kolme ominaispiirrettä jotka ovat, **kehittäminen syntyy tarpeesta muutokseen**, **kehittäminen johtaa käytettävään tuotokseen** ja **kehitys tuottaa edistävää tietoa**. (Pernaa 2013.)

Tutkimusaineiston hankkimisessa käytettiin osittain laadullisen tutkimuksen aineistonkeruumenetelmiä, jotka sisältävät haastatteluja, havainnointia sekä valmiita aineistoja (Järvenpää 2006). Aineistoa kerättiin uusista ja luotettavista lähteistä. Lähteisiin vaikutti myös opinnäytetyön aiheena olevan ratkaisun tuoreus, joka rajasi valmiiden aineistojen hyödyntämistä. Havainnointia tehtiin jatkuvasti työn edetessä ja Yritys X:n ohjaajan asiantuntijuutta hyödynnettiin erilaisissa teknisissä asioissa.

3 Teoriaosuus

3.1 VPN-tekniikka

Virtual Private Network (VPN) on tekniikka, jonka avulla yritykset ja käyttäjät pystyvät kuljettamaan tietoliikennettään julkisen verkon yli turvallisesti. Sen avulla mahdollistetaan etäyhteys, etäohjaus ja korkea suojaus liikenteelle yksityisessä verkossa. Tekniikasta puhutaan tunnelointiyhteytenä verkkolinkkien välillä. (Stewart 2014a.)

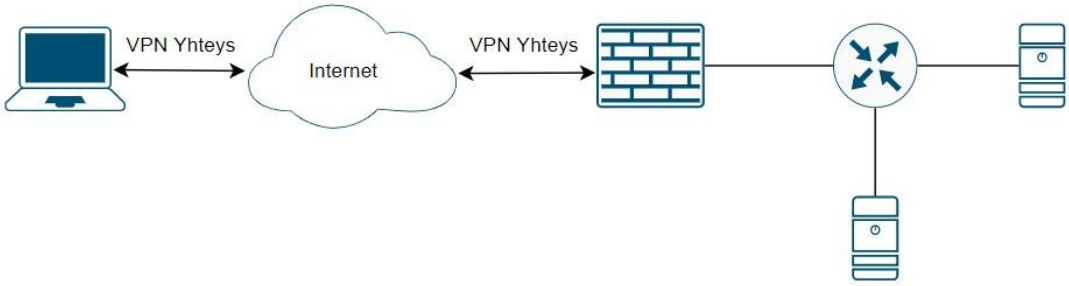
Etäyhteys mahdollistaa organisaation resursseihin pääsyyn yrityksen verkon ulkopuolelta, eli se luo paikallisverkon linkin järjestelmälle, joka ei todellisuudessa ole fyysisesti lähellä verkkoa. Useasti etäyhteys luodaan käyttäjältä takaisin ensisijaiseen verkkoon, mutta jos käyttäjän täytyy olla yhteydessä yrityksen lähiverkkoon, käytetään Remote Access Server (RAS) palvelimia yhteyksien hyväksymiseen. Jos etäyhteyden käyttäjä pystyy yhdistämään lähiverkkoon oman verkkoyhteyden avulla, paikallinen verkkoyhteys on välttämätön. Kun verkkoyhteys on kytketty, VPN-yhteys voidaan muodostaa ja etäyhteyden käyttäjä voi käyttää verkossa olevia resursseja, kuin se olisi paikallisesti kytketty. (Stewart 2014a.)

VPN-yhteyksien turvallisuuteen ei varhaisessa vaiheessa kiinnitetty huomiota, vaan keskityttiin tunnelointi- ja kapselointiprosesseihin. Nykyisin on erittäin tärkeää, että VPN-yhteys on todennettu ja salattu. Turvallisen etäyhteyden näkökulmasta kaikki VPN-liikenne on oltava todennettua ja salattua, sillä VPN ilman todennusta ei ole yksityinen. Tämän lisäksi kaikkien VPN-päätepisteiden tulisi noudattaa samoja turvallisuusparametreja sekä algoritmeja. VPN-tunneleissa täytyy myös olla vastaavat salausavainsarjat, mikä mahdollistaa, että salatun liikenteen kulku voidaan toteuttaa turvallisesti. Oikeiden salausprotokollien käyttäminen on myös tärkeää, sille ne varmistavat etteivät ulkopuoliset osapuolet voi vaikuttaa etäyhteyden turvallisuuteen. Huono salaus tekee muuten turvallisesti toteutetusta etäyhteydestä huonon, ja siksi se on ehdottoman tärkeä ottaa huomioon. (Stewart 2014a.)

3.2 VPN-tyypit

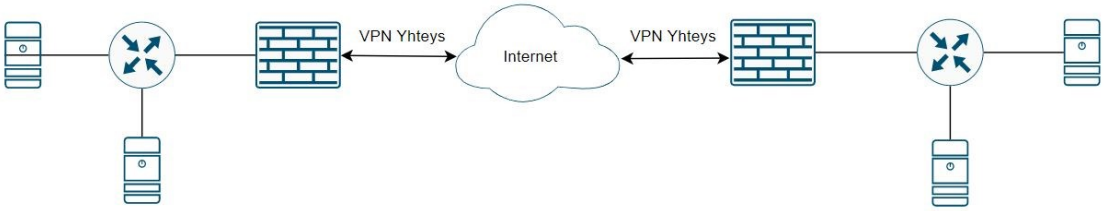
Kun puhutaan VPN-yhteyksistä, on olemassa kaksi yleistä toteutustapaa. Näitä kutsutaan VPN-tyypeiksi. Erona näillä toteutustavoilla on niiden käyttötarkoitus.

Host – to – Site VPN-yhteyttä (ks. Kuvio 1) kutsutaan myös nimellä remote access VPN. Yhteystyyppi tukee yhtä isäntäyhteyttä lähiverkkoon. Tällä mahdollistetaan yksittäiselle käyttäjälle helppo pääsy yksityiseen lähiverkkoon, joka tukee useita etäkäyttäjiä usealla VPN-päätelaitekonseptilla. (Stewart 2014b.)



Kuvio 1. Host-to-Site VPN (Stewart 2014b, muokattu)

Toinen yleisesti tyypeistä on **Site-to-Site** (ks. Kuvio 2), joka oikein toteutettuna toimii halpana keinona toteuttaa hajautettu lähiverkko esimerkiksi yrityksen toimipisteiden välillä. Tarkemmin kuvailtuna ratkaisua kutsutaan lähiverkkojen välisiksi VPN-verkoiksi tai lähiverkkojen välisiksi WAN VPN-yhteyksiksi. Ratkaisu tukee suojattuja yhteyksiä lähiverkkojen välillä julkisten välittäjäverkkojen välityksellä. (Stewart 2014b.)



Kuvio 2. Site-to-Site VPN (Stewart 2014b, muokattu)

3.3 VPN-protokollat

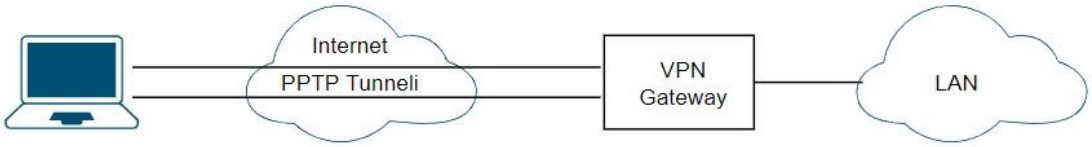
Koska VPN-viestintä tapahtuu julkisessa verkossa, ennen varsinaista tiedonsiirtoa molempien osapuolien tulisi tietää, kuinka he kommunikoivat turvallisesti. Turvallisen kommunikoinnin periaatteisiin kuuluu, miten tiedot salataan ja kuinka salausavaimien vaihto tapahtuu. Näin voidaan varmistaa, että tietoja välitetään turvallisesti. (Nayak & Rao 2014.)

Vaiheita VPN-yhteyksillä on kaksi, joista ensimmäisessä muodostetaan suojattu yhteys osapuolten välillä, jolloin varmistetaan, että molemmat osapuolet ovat aitoja ja samalla tehdään salausavaimien vaihto. Salausavaimen vaihto tehdään tietojen salaamisen, salauksen purkamisen ja tiedon eheyden tukemiseksi. Kun molemmat osapuolet tietävät avaimet, alkaa toinen vaihe, jolloin varsinainen tiedonsiirto tapahtuu salattuna. (Nayak & Rao 2014.)

VPN-protokollien tulisi tukea tunnelointia, tietojen todennusta, tietojen eheyttä, tietojen salausta ja toistojen estoa, jotta suojattu yhteys voidaan muodostaa. Tunnelointi tarkoittaa yhden datapaketin kapselointia toiseen datapakettiin, eli yhden protokollan datapaketti lisätään toiseen protokollaan, jonka jälkeen se siirretään käyttäjän ja palvelimen välillä. Tietojen todennus varmentaa osapuolten aitouden ja että vastaanotetut tiedot ovat aidolta käyttäjältä. Tietojen eheydellä varmistetaan, ettei tietoa ole muokattu tiedonsiirron aikana. Tietojen salaus julkisessa verkossa varmistaa tietojen luottamuksellisuuden ja yksityisyyden suojaamisen. Toistojen estoilla tarkoitetaan palveluita, joilla voidaan hylätä pakettien kaksoiskappaleet tai paketit, jotka saapuvat myöhässä, sillä niitä voidaan käyttää toistohyökkäyksiin. (Nayak & Rao 2014.)

Point-to-Point Tunneling Protocol (PPTP) on tunnelointiin käytetty VPN-protokolla (ks. Kuvio 3), joka hallitsee käyttäjien todennusta, tietojen eheyttä sekä tietojen salausta. PPTP pohjautuu PPP-protokollaan. PPP on tiedonsiirtoprotokolla, jota käytetään suoran yhteyden muodostamiseen verkkolaitteiden välillä. Käyttäjien todentaminen tapahtuu ennen tiedonsiirtoa. Protokolla mahdollistaa siis PPP:n tunneloimisen verkossa. GRE on osa protokollaa ja sitä käytetään PPP-paketin kuljettamiseen

verkossa. PPTP tukee PAP, CHAP, MS-CHAPv1 ja MS-CHAPv2 todennusmenetelmiä. (Nayak & Rao 2014.)

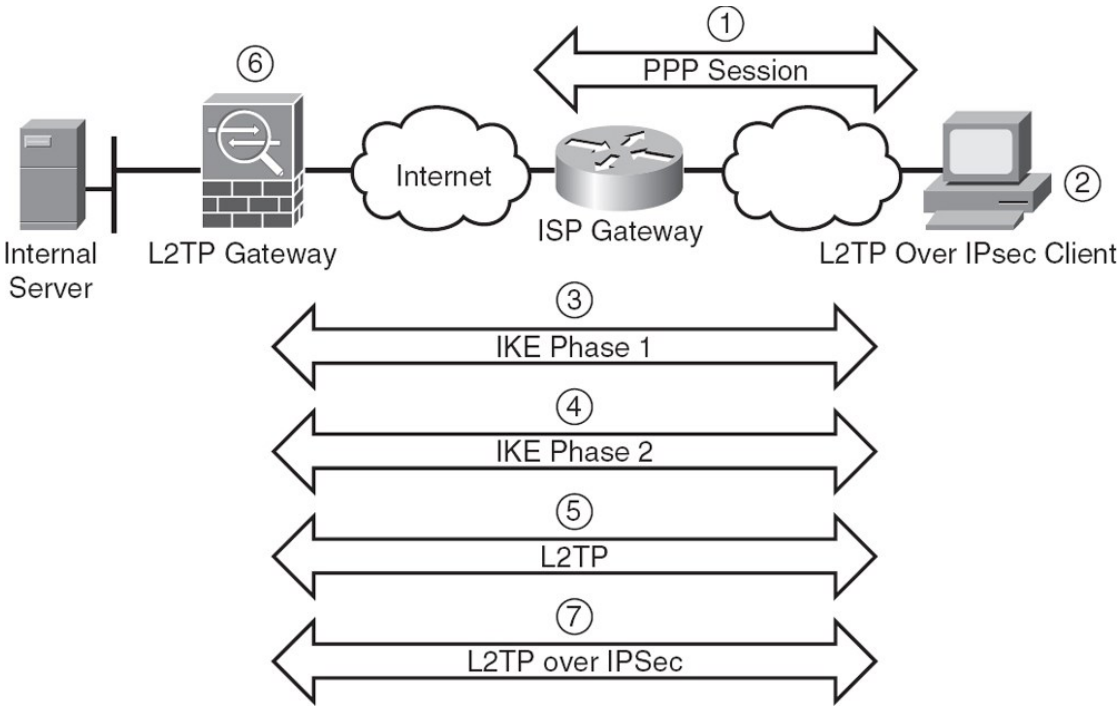


Kuvio 3. PPTP-tunneli (Rao & Nayak 2014, muokattu)

Layer 2 Tunneling Protocol (L2TP) yhdistää PPTP-protokollan sekä Ciscon L2F-protokollien ominaisuudet ja siksi se onkin PPTP-protokollan lisä. Sen tarkoituksena on tarjota yhteyden läpinäkyvyyttä kahden käyttäjän ja sovellusten välillä. L2TP sallii Layer 2-protokollan ja PPP-protokollan kommunikoinnin keskenään laajentamalla PPP-mallia. (Nayak & Rao 2014.)

Suurin osa L2TP-toteutuksista käyttää IPSec-tietoliikenneprotokollaa, sillä L2TP ei yksin tarjoa vahvaa tietojen luottamuksellisuutta (Rao & Nayak 2014). IPSec on Layer 3-protokolla, jonka tarkoituksena on suojata IP-paketit kerroksessa 3 ja siitä korkeammissa kerroksissa. Tietojen eheyden ja niiden todentamisen IPSec tekee HMAC-toimintojen avulla. Tietojen luottamuksellisuuden varmentaminen tapahtuu salausalgoritmeilla, jonka lisäksi IPSec määrittelee pakettien kentät, sekä miten paketit kuljetetaan, eli joko tunnelimuodossa tai kuljetusmuodossa. Tunnelimuotoa käytetään Site-to-Site ja Host-to-Site yhteyksille. Tässä muodossa IPSec suojaa alkuperäisen paketin kokonaan. Kuljetusmuotoa käytetään myös tiettyihin point-to-point yhteyksiin. (Deal 2006.)

L2TP IPSec toteutuksessa käyttäjä ja tietoturvalaite käyvät läpi seitsemän vaihetta (ks. Kuvio 4).



Kuvio 4. L2TP IPSec (Frahim & Santos 2010.)

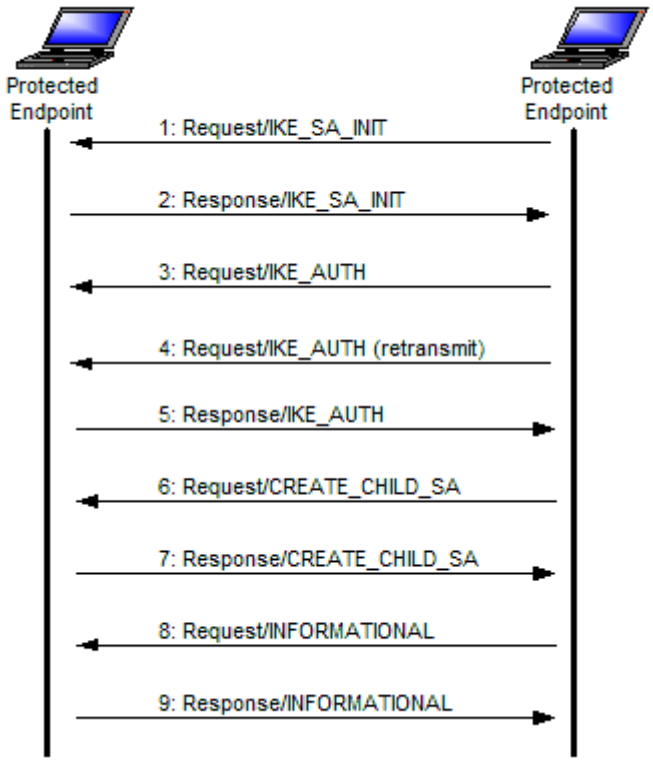
1. Ensimmäisessä vaiheessa käyttäjä muodostaa PPP-istunnon palveluntarjoajan reitittimelle ja vastaanottaa dynaamisen julkisen IP-osoitteen. Jos työasemalla on jo olemassa IP-osoite ja sitä voidaan käyttää, on tämä vaihe ylimääräinen.
2. Toisessa vaiheessa käyttäjä käynnistää L2TP ohjelman, johon määritetty käyttöön IPSec.
3. Kolmannessa vaiheessa työasema aloittaa istunnon sekä neuvottelee kanavan avainten vaihtamiseen. Tästä vaiheesta puhutaan myös IPSec:n ensimmäisen vaiheen neuvotteluna.
4. Kun kolmas vaihe on suoritettu onnistuneesti, voidaan aloittaa neljäs vaihe, jossa käyttäjä perustaa kaksi suojattua kanavaa tietojen salaamista ja todentamista varten. Vaiheesta puhutaan myös nimellä IPSec:n toisen vaiheen neuvotteluna.
5. Viidennessä vaiheessa, kun IPSec on muodostettu, käyttäjä voi aloittaa L2TP-istunnon IPSec:n sisällä.
6. Kuudennessa vaiheessa käyttäjän todennustietoja käytetään vahvistamaan L2TP-istunto. Kun käyttäjän todennus on onnistunut, PPP- tai L2TP-määrityksistä neuvotellaan.
7. Seitsemännessä vaiheessa, kun L2TP-istunto on muodostettu, käyttäjän työaseman lähettämä liikenne on kapseloitu L2TP:n sisään. L2TP-paketit on salattu IPSec protokollalla ja tämän jälkeen lähetetty tunnelin toiseen päähän internetin välityksellä. (Frahim & Santos 2010.)

Internet Key Exchange version 2 (IKEv2) on IPsec VPN-protokollaan perustuva standardipohjainen avaimenhallintaprotokolla. IKEv2 on paranneltu versio IKE-protokollasta ja se tukee korkeinta mahdollista salausta etäyhteyksien käyttäjille. Se on lisäksi yhteensopiva useiden VPN-laitteiden kanssa (Hicks 2019). IKEv2 käyttämä salaus hyödyntää useita salausprotokollia, jotta kaikki avaintenhallinnan turvallisuusmääritykset voidaan suorittaa. Protokolla perustuu Diffie-Hellman avaimenhallintaprotokollaan. (Internet Key Exchange version 2 (IKEv2) Protocol n.d.)

Protokolla muodostaa ja ylläpitää jaettua tilaa IP-datagrammien päätepisteiden välillä, jonka lisäksi se suorittaa keskinäisiä todennuksia kahden osapuolen välillä ja perustaa IKEv2-tietoturvayhdistyksen, josta käytetään myös nimeä SA. IKE-SA tekee kaksi erilaista toimintoa, joihin se käyttää tallentamiaan jaettuja salaisia tietoja. Nämä kaksi toimintoa ovat perustaa CHILD-SA ESP-protokollalle tai AH-todennusotsikolle ja määrittää salausalgoritmit, joita SA:t käyttävät. (Internet Key Exchange version 2 (IKEv2) Protocol n.d.)

IKEv2 käyttää pareja vaihtoina, eli se on pyyntö/vastaus pari protokolla. Pyynnön esittäjän täytyy varmistaa luotettavuus, joten jos vastausta ei saada, pyynnön esittäjä joko hylkää yhteyden tai lähettää sen uudelleen. Yhteensä IKEv2 käyttää neljän tyyppisiä vaihtoja. Nämä ovat IKE_SA_INIT, joka on ensimmäinen vaihto. Vaihdon tarkoituksena on perustaa IKE-SA ja tämän täytyy tapahtua täydellisesti, jotta muita vaihtoja voi tapahtua. IKE_SA_INIT muun muassa neuvottelee IKE-SA suojausparametrit ja lähettää Diffie-Hellman arvot. Seuraavaksi tapahtuu toinen vaihto, joka on IKE_AUTH. IKE_AUTH lähettää identiteettejä ja osoittaa niihin liittyvät salaukset. Sen tarkoituksena on myös perustaa ensimmäinen ja yleisesti samalla ainoa AH ja/tai ESP CHILD-SA. Nämä kaksi ensimmäistä vaihtoa ovat pakollisia ja kun ne on saatu suoritettua loppuun järjestyksessä, seuraavaksi tapahtuvat vaihdot voivat tapahtua missä tahansa tarpeen mukaisessa järjestyksessä. Joissakin tapauksissa näitä vaihtoja ei tarvitse tehdä ollenkaan. Toinen lopuista vaihdoista on CREATE_CHILD_SA, joka pystyy luomaan tarvittaessa lisää CHILD-SA määrityksiä. Viimeinen vaihto on INFORMATIONAL, joka on niin sanotusti huoltovaihto, joka ylläpitää SA:ita. Joitakin

ominaisuuksia tälle vaihdolle ovat, SA:n poisto tarvittaessa, virheolosuhteiden ilmoitukset ja SA:n toimivuuden tarkastus. (Internet Key Exchange version 2 (IKEv2) Protocol n.d.) Esimerkki IKEv2 vaihdoista (ks. Kuvio 5).

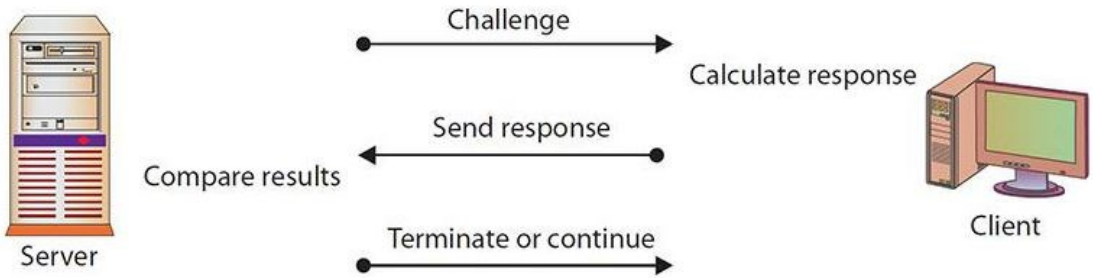


Kuvio 5. IKE-vaihdot (Internet Key Exchange version 2 (IKEv2) Protocol n.d.)

3.4 Todennusprotokollat

Password Authentication Protocol (PAP) käyttää linkin muodostamiseen yksinkertaista kaksivaiheista kättelyä. Tämä tarkoittaa, että käyttäjä lähettää käyttäjänimen ja salasanan palvelimelle, joka hyväksyy tai hylkää todennuksen. PAP todennusmenetelmää käytettäessä salasanat lähetetään linkin välityksellä selkeänä tekstinä, eikä niitä suojata pakettien toistohyökkäyksiltä. (Nayak & Rao 2014.)

Challenge-Handshake Authentication Protocol (CHAP) toimii kolmivaiheisen kättelyn avulla (ks. Kuvio 6), joka tarkoittaa, että linkin muodostamiseen palvelin lähettää aluksi haasteviestin käyttäjälle, johon käyttäjä vastaa yksisuuntaisella hashilla. Jos käyttäjän vastaus täsmää, todennus kuitataan ja yhteys muodostetaan. Muussa tapauksessa yhteys katkaistaan. CHAP suojaa pakettien toistohyökkäyksiltä ja hallitsee myös haasteiden taajuutta, sekä ajoituksia. (Nayak & Rao 2014.)



Kuvio 6. Kolmivaiheinen kättely (Conklin, Cothren, Davis, White & William 2018.)

Extensible Authentication Protocol (EAP) on yleisesti käytetty todennuskehys, jota käytetään useasti PPP-yhteyksissä ja langattomissa verkoissa. Vaikka sen käyttö tapahtuu usein langattomissa lähiverkoissa, sitä voidaan käyttää myös langallisissa todennuksissa. (Conklin, Cothren, Davis, White & William 2018.) EAP protokollaa käytetään PPP:n käyttämien todennusprotokollien laajentamiseen. Se tukee useita todennusmekanismeja, joita ovat esimerkiksi, tokenit, varmenteet, älykortit, kertakäyttöiset salasanat ja julkisen avaimen salauksen todennukset. (Rouse 2005.)

Protokolla on otettu käyttöön Windowsin työasemien sisäänrakennetussa VPN-ratkaisussa tukemaan vanhempia ja vähemmän käytettyjä salasanapohjaisia todennusmenetelmiä. Tällä voidaan varmistaa suojattu todennus käyttäjänimelle ja salasanalle sekä varmennepohjaisille menetelmille. (VPN authentication options 2017.)

Protected Extensible Authentication Protocol (PEAP) on protokolla, jonka toiminta perustuu EAP viestintäkanavien suojaamiseen. Sen tarkoituksena on tarjota suojaus kuljetuskerroksessa EAP:n sisällä, johon se käyttää julkisen avaimen salausvarmennetta. Palvelinten osalta julkisen avaimen varmenteita käytetään palvelinten todentamiseen. (Protected Extensible Authentication Protocol (PEAP) n.d.)

Yleisin tarkoitus PEAP protokollalla on puuttua tietoturvahäiriöihin tietynlaisissa todennuskehyksissä ja estää erityyppisiä tietomurtoja järjestelmään, jotka voivat aiheuttaa ongelmia 802.11 verkkoliikenteessä. PEAP takaa varman ja turvallisen todennuksen. (Protected Extensible Authentication Protocol (PEAP) n.d.)

3.5 Käytössä oleva etäyhteystekniikka

Tuotantoympäristössä käytössä oleva Direct Access on etäyhteysratkaisu, joka esiteltiin ensimmäisen kerran osana Windows Server 2008 R2 käyttöjärjestelmää. Sen tarkoituksena on muodostaa yhteys automaattisesti yrityksen verkkoon, aina kun käyttäjälaite on yhteydessä verkkoon yrityksen verkon ulkopuolelta. Yhteyden tulee olla suojattu ja todennettu. Direct Access yhteyksien muodostaminen tapahtuu koneiden toimesta, eli käyttäjän ei itse tarvitse muodostaa yhteyttä. Järjestelmänvalvojille Direct Access antaa mahdollisuuden hallita etäyhteydessä olevia käyttäjiä, jota voidaan hyödyntää useissa eri tilanteissa. (Hicks 2016.)

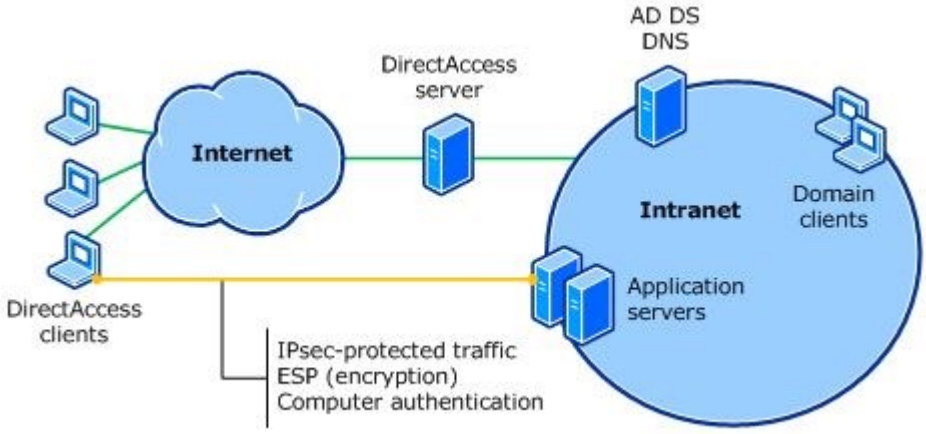
Direct Access on myös turvallinen tapa toteuttaa etäyhteys, sillä käyttäjien laitteiden täytyy olla toimialueeseen liitettyjä ja useasti myös omistaa sertifikaatti, jonka on myöntänyt yrityksen PKI. Näiden kahden toimenpiteen avulla voidaan taata korkeampi varmuustaso etäyhteyksille, joka on luonnollisesti jokaisen yrityksen päämäärä. (Hicks 2016.)

Palvelimien osalta Direct Access on tuettu Windows Server 2008 R2, Windows Server 2012 ja Windows Server 2016 käyttöjärjestelmissä. Työasemien osalta tuettuina vaihtoehtoina ovat Windows 7, Windows 8 ja Windows 10 käyttöjärjestelmät. Kokonaisuutena Direct Access on siis tuettu laajasti eri käyttöjärjestelmillä, mikä takaa joustavuutta laitekokoonpanoissa ja toteutuksissa. (DirectAccess 2020.) Direct Access asetuksien määritys työasemille tehdään GPO:n avulla, joka suoritetaan ainoastaan koneille, jotka ovat määritetyn turvallisuusryhmän (security group) jäseniä. Turvallisuusryhmä määritellään etäyhteyden konfiguroinnin yhteydessä. (Step 1 Configure Advanced DirectAccess Infrastructure 2020.)

Yksi tärkeimmistä asioista Direct Access ympäristöissä on NLS, joka on web-palvelin, johon on asennettu SSL-varmenne. Sen avulla määritellään ovatko käyttäjät yrityksen verkossa vai sen ulkopuolella ja tämän takia palvelin ei saa olla saavutettavissa julkisesta verkosta. Laite, jonka käyttöön Direct Access on määritetty, testaa ensimmäisenä yhteyttä NLS-palvelimeen käynnistyessään tai verkkoliitäntöjen vaihtuessa. (Hicks 2015.)

Turvallisen yhteyden luomiseksi käyttäjän ja yrityksen sisäverkon välille Direct Access hyödyntää IPv6-protokollaa osana IPSeciä. Liitettävyyttä IPv6-verkkoon tai sen tukemista sisäisissä verkoissa ei kuitenkaan edellytetä, vaan Direct Access sen sijaan käyttää IPv6-siirtotekniikoita automaattisesti tunneloimaan IPv6-liikenteen IPv4-verkoissa. Kyseisiä tunnelointitekniikoita ovat 6to4, Teredo ja IP-HTTPS. IPv4-sisäverkossa tunnelointi toteutetaan NAT64 tai ISATAP tekniikoiden avulla. (Step 1 Plan the Advanced DirectAccess Infrastructure 2020.)

Esimerkkinä käytetään päästä päähän (end-to-end) toteutusta (ks. Kuvio 7), jossa kaikki liikenne käyttäjältä sisäverkkoon on päästä päähän menetelmällä toteutettu ja salattu IPsecin avulla. Direct Access-palvelin toimii läpikulkulaitteena, sallien IPsec-suojatun liikenteen sovelluspalvelimille. (End-to-end Access Example 2012.)



Kuvio 7. Direct Accessin suunnitteluesimerkki (End-to-end Access Example 2012.)

4 Always On VPN -etäyhteystekniikka

Monen tunteman Direct Access etäyhteyden seuraaja Always On VPN tarjoaa tuttuun tapaan automaattisia VPN-yhdistysprofiileja, jotka mahdollistavat täysin automaattisen käyttökokemuksen loppukäyttäjille. Sen ideana on tarjota samanlainen käyttökokemus, kuin Direct Access, mutta tällä kertaa entistä turvallisempana ja helpommin lähestyttävänä konfiguroinnin näkökulmasta. Always On VPN käyttää perinteisiä VPN-protokollia, kuten IKEv2, SSTP ja L2TP/IPSec. Tämän lisäksi se mahdollistaa uusien ominaisuuksien käytön, joita ovat muun muassa ehdollisen pääsy (conditional access), Windows Hello yrityksille, Azure pilviympäristön hyödyntäminen laite/profiilihallinnassa sekä multifactor todennuksissa. Muita ominaisuuksia ovat WIP-integraatio, liikennesuodattimet VPN-verkon käytön rajoittamista varten ja sovelluksien käyttöön perustava VPN-yhteyden luonti. (Hicks n.d.)

Always On VPN tukee toimialueeseen, verkkotunnuksilla (workgroup) tai Azure AD:hen liitettyjä laitteita sekä mahdollistaa jopa henkilökohtaisesti omistettujen laitteiden liittämisen. Yhteystyyppi voi vaihdella, eikä sen tarvitse olla yksin käyttäjä tai laite, vaan se voi olla niiden yhdistelmä. Mahdollista on toteuttaa esimerkiksi laitteen etähallinta laitetodennuksella ja yhteys yrityksen sisäisiin resursseihin käyttäjätodennuksen avulla. (Always On VPN deployment for Windows Server and Windows 10. n.d.)

Always On VPN tuo mukanaan etuja ja myös haittoja. Etuina ovat tuki myös muille, kuin Enterprise Windows 10 asiakkaille, eli käytön mahdollisuus Windows 10 Home ja Professional käyttöjärjestelmillä. Etäyhteysratkaisu voi käyttää joko IPv4 tai IPv6 protokollaa, jonka lisäksi se on infrastruktuuri riippumaton. Windows RRAS tuen lisäksi on mahdollista käyttää mitä tahansa kolmannen osapuolen verkkolaitetta. (Hicks n.d.)

Haittana on se, että ratkaisua ei voi toteuttaa muulle, kuin Windows 10 käyttöjärjestelmälle, sillä sitä ei tueta Windows 7:ssä. Tämän lisäksi sen hallintaan on tapahtunut muutoksia, joiden takia sitä ei voi hallita suoranaisesti enää Active Directoryn tai ryhmäkäytänteiden (group policy) avulla. Määritys ja hallinta on mahdollista toteuttaa

jollakin seuraavista, Microsoft Intune, Microsoft System Center Configuration tai Powershell. (Hicks n.d.)

Tämän etäyhteysratkaisun julkistaminen on herättänyt kysymyksiä, kannattaako ratkaisu toteuttaa nyt vai hyödyntää esimerkiksi Direct Access toteutusta. Always On VPN on tulevaisuuden ratkaisu, jota tullaan varmasti käyttämään Direct Access yhteyden seuraajana, kun sen tuki lopulta päätetään. Direct Access tulee olemaan tuettu koko Windows Server 2019 elinkaaren, joten varsinaista pakottavaa tarvetta uuden Always On VPN ratkaisun käyttöönotolle ei ole. Jos kuitenkin tarvittavat vaatimukset uudelle ratkaisulle löytyvät, on se hyvä vaihtoehto tulevaisuutta ajatellen. (Hicks n.d.)

4.1 Ominaisuudet ja toiminnot

Etäyhteysratkaisulla on useita erilaisia ominaisuuksia ja toimintoja, joista käydään läpi yleisimpiä. Läpinäkyvään ja saumattomaan yhteyteen Always On VPN hyödyntää automaattista laukaisua, joka perustuu sovelluksen käynnistymiseen tai nimitilan tarkkuuspyyntöihin. (Always On VPN features and functionalities 2018.)

VPN-profiilien laitetunnelin avulla voidaan saavuttaa erillisen infrastruktuuritunnelin käyttö yhteyksien tarjoamiseksi käyttäjille, jotka eivät ole kirjautuneet yrityksen verkkoon. Laitetunneli on mahdollista määrittää ainoastaan verkkotunnuksella liitettyihin (domain-joined) laitteisiin, jotka hyödyntävät IKEv2 laitevarmenteen todennusta. Laitetunnelia voidaan myös hyödyntää etäyhteyksille yrityksen verkosta käyttäjän laitteelle. (Always On VPN features and functionalities 2018.)

Automaattista tunnelityyppiä voidaan käyttää takaisinpaluussa IKEv2:sta SSTP:hen. Tätä käytetään yleensä, kun käyttäjät ovat palomuurien tai välityspalvelimien takana. Tämä on mahdollista käyttäjätunnelissa, joka tukee SSTP:tä ja IKEv2:ta, mutta ei laitetunnelissa, sillä se tukee ainoastaan IKEv2 protokollaa. (Always On VPN features and functionalities 2018.)

Yrityksen resursseihin pääsy mahdollistetaan käyttämällä tunnelikäytäntöjä, jotka vaativat todennuksen ja salauksen, kunnes ne saavuttavat VPN-yhdyskäytävän. Oletuksena tunneli-istunnot päättyvät VPN-yhdyskäytävään, joka toimii samalla IKEv2-yhdyskäytävänä. Tämä tarjoaa suojauksen niin sanotusti reunasta reunaan (end-to-edge). (Always On VPN features and functionalities 2018.)

IKEv2 protokolla, joka on osa Always On VPN alustaa, tukee erityisesti laite- ja tietokonevarmenteita VPN-todennuksessa. Tästä johtuen Always On VPN tarjoaa tuen konevarmenteiden todennukselle. (Always On VPN features and functionalities 2018.)

Etäyhteysmahdollisuus voidaan rajoittaa vain joillekin käyttäjille tai käyttäjäryhmille. Tämä on mahdollista toteuttaa käyttämällä RADIUS:ta VPN-yhteyksien hallitsemiseksi. (Always On VPN features and functionalities 2018.)

Mahdollisuudet havaita yrityksen verkkoyhteydet, joka perustuu verkkorajapinnoille ja verkkoprofiileille osoitettujen DNS-päätteiden arviointiin. Näin on siis mahdollista määrittää tarvittaessa intranet-yhteys, kun laite on kytketty yrityksen verkkoon. (Always On VPN features and functionalities 2018.)

4.2 Parannukset

Aikaisempiin Windows VPN-ratkaisuihin Always On VPN tuo monia etuja, jotka kohdistuvat Microsoftin cloud-first ja mobile-first visioon. Alustaintegraatiossa on parannettu integraatiota Windows käyttöjärjestelmiin sekä kolmansien osapuolien ratkaisuihin. Näin varmistetaan laaja tuki monille yhteydenottotavoille. (Always On VPN enhancements 2018.)

Suojauksen osalta Always On VPN hyödyntää uusia ja edistyneitä tietoturvaominaisuuksia. Näin voidaan rajoittaa liikennetyyppejä, määrittää sovellukset jotka voivat käyttää VPN-yhteyttä ja valita käytettävät todennusmenetelmät yhteyksien muodostamiselle. Yhteyden turvallisuus on ensisijaisen tärkeää, varsinkin yhteyksissä, jotka ovat lähes aina käytössä. (Always On VPN enhancements 2018.)

VPN-yhteyksien osalta ennen ei ollut mahdollista luoda automaattista yhteyttä laitteen tai käyttäjän todennuksen avulla. Always On VPN mahdollistaa automaattisen laukaisun, joko laitetunnelilla tai ilman. (Always On VPN enhancements 2018.)

Verkkojenhallinta Always On VPN ratkaisussa antaa järjestelmänvalvojien tehdä yksityiskohtaisempia määrityksiä reitityskäytänteisiin tai jopa yksittäiseen sovellukseen. Täysi yhteensopivuus IPv4 ja IPv6 protokolliin takaa, että riippuvuutta pelkkään IPv6 protokollaan ei ole, kuten Direct Access ratkaisuissa. Käyttöönotto ja hallinta voidaan toteuttaa useilla eri tavoilla, joka tuo paljon etuja Always On VPN ratkaisulle. (Always On VPN enhancements 2018.)

4.3 Todennusvaihtoehdot

Mahdollisia todennusvaihtoehtoja ovat EAP-MSCHAPv2, joka perustuu käyttäjätunnuksen ja salasanan todentamiseen tai Winlogon-käyttäjätietoihin, joka pystyy määrittelemään todennuksen tietokoneen sisäänkirjautumistiedoilla. (VPN authentication options 2017.)

EAP-TLS, joka tukee varmenteiden todennuksia, suodatusta sekä palvelimen varmentamista. Varmenteiden todennuksissa tuetaan varmenteita avaimilla KSP ja TPM ratkaisuissa. Näiden lisäksi tuetaan älykortti varmenteita ja Windows Hello for Business varmenteita. Varmenteiden suodatusta käytetään, kun halutaan etsiä jokin tietty varmenne todentamista varten. Suodatus perustuu tehostettuun avainkäyttöön (EKU). Palvelinten varmentamiseen käytetään palvelimen nimeä, palvelinvarmennetta ja ilmoitusta, jossa voidaan kysyä, luotetaanko palvelimeen vai ei. (VPN authentication options 2017.)

PEAP, jonka avulla voidaan suorittaa palvelimen varmentaminen ja tarvittaessa ottaa se pois käytöstä. Mahdollisuus käyttää sisäistä menetelmää on myös käytettävissä. Sisäinen menetelmä tarkoittaa, että ulkoinen menetelmä luo turvallisen tunnelin, jonka loppuun todentamisessa käytetään sisäistä menetelmää. Näitä voivat olla EAP-MSCHAPv2 tai EAP-TLS. PEAP mahdollistaa myös nopean uudelleenyhdistämisen, joka vähentää viivettä käyttäjän todennuspyynnön ja NPS-palvelimen tai RADIUS-

palvelimen suorittaman vastauksen todentamisen välillä. Näin voidaan vähentää käyttäjän ja palvelimen resurssivaatimuksia, sekä minimoida valtuutustietojen lähettämisen kertoja. Lisäksi PEAP sisältää ”salauksen sitomisen”, jonka avulla PEAP-neuvottelut suojataan Man in the Middle hyökkäyksiltä. (VPN authentication options 2017.)

TTLS, joka käyttää sisäistä menetelmää ja palvelimen todennusta, kuten PEAP. Erona on että palvelin täytyy todentaa TTLS vaihtoehdossa. Palvelimen todentamiseen voidaan määrittää palvelimen nimi, luotettu juurivarmenne palvelinvarmenteelle ja ilmoitus luotetaanko palvelimeen vai ei. (VPN authentication options 2017.)

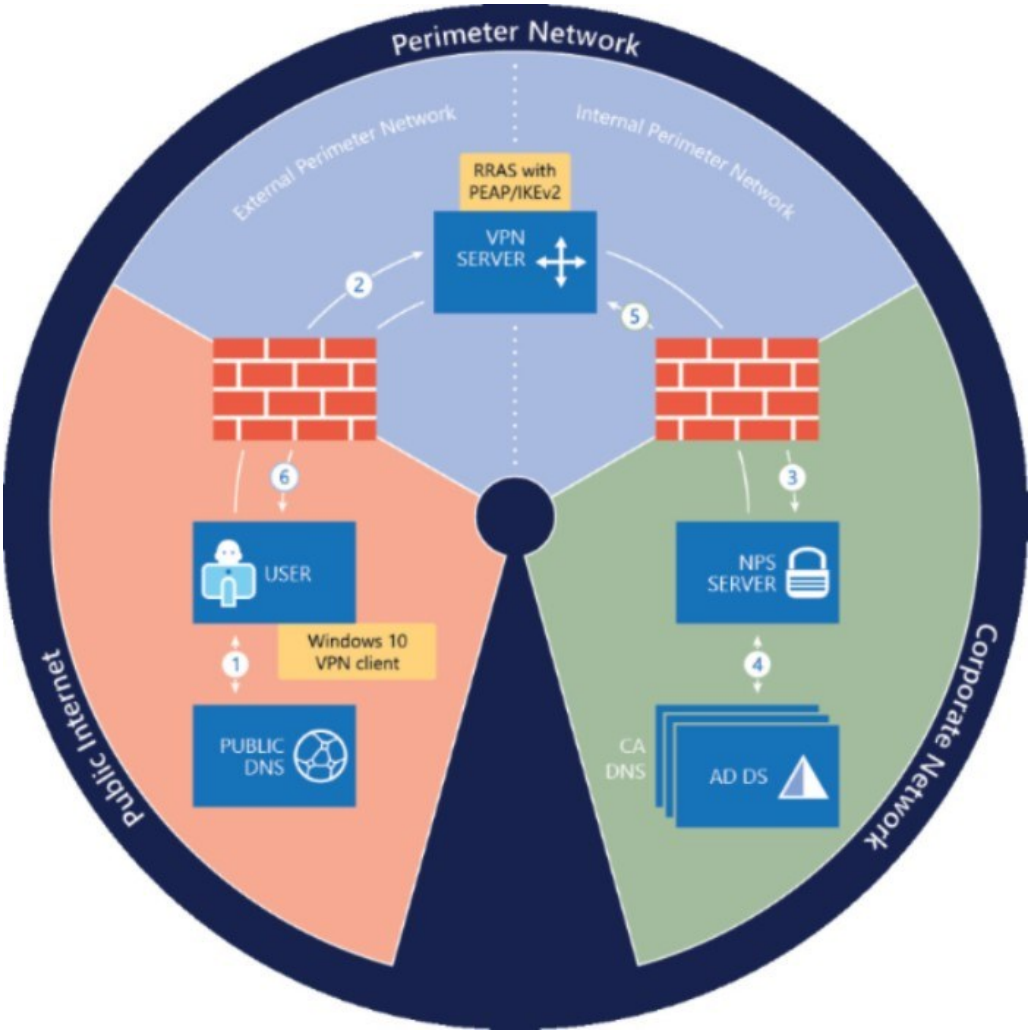
4.4 Toimintaperiaate

Useimmat infrastruktuurit käyttävät jo ennestään tekniikoita, joilla Always On VPN on mahdollista toteuttaa, mutta on mahdollista, että muutoksia ja lisäyksiä täytyy tehdä käyttöönoton yhteydessä. Yleisesti Always On VPN tarvitsee DC/DNS palvelimen tai palvelimet, NPS (RADIUS) palvelimen, CA palvelimen sekä palvelimen etäkäyttöä varten, joka on RAS (RRAS/VPN). Käyttöönottoa varten ei vaadita, että AD DS, AD CS tai NPS-palvelimissa on käytössä Windows Server 2016, vaan aiempien versioiden, kuten Windows Server 2012 R2 käyttö on mahdollista. (Always On VPN deployment for Windows Server and Windows 10 n.d.)

Palvelinten tarkempia määreitä

Käyttöönottoon tarvitaan Active Directory ympäristö, joka sisältää yhden tai useamman DNS-palvelimen. Sisäinen ja ulkoinen DNS-vyöhyke vaaditaan, mistä oletetaan, että sisäinen vyöhyke on ulkoisen vyöhykkeen subdomain. Julkisen avaimen infrastruktuuri, eli PKI, joka pohjautuu Active Directoryyn ja tämän lisäksi varmennepalvelut, eli AD CS. NPS-palvelin, joka määrittelee verkkopolitiikat. NPS-palvelin voi olla fyysinen tai virtuaalinen. Olemassa olevaa NPS-palvelinta on mahdollista muokata uuteen ratkaisuun sopivaksi, uuden asentamisen sijaan. VPN-palvelin, joka toimii RAS-yhdyskäytävänä. VPN-palvelimelle tarvitaan ainoastaan ominaisuudet IKEv2 VPN-yhteyksien tukemiselle ja lähiverkon reititykseen. (Always On VPN deployment for Windows Server and Windows 10 n.d.)

Kehysverkko, johon tulisi oikeaoppisessa toteutuksessa sijoittaa kaksi palomuuria, jotka sallivat VPN- ja RADIUS-tiedonsiirron. VPN-palvelin tulisi sijoittaa näiden kahden palomuurin väliin. Palvelinten varsinaiset sijoittamiset voivat vaihdella toteutustapojen mukaan ja tämä on yksi tapa toteuttaa käyttöönotto. (Always On VPN deployment for Windows Server and Windows 10 n.d.). Kehysverkosta ja palvelinten sijoittaminen (ks. Kuvio 8).



Kuvio 8. Always On VPN:n käyttöönotto (Always On VPN technology overview 2018.)

Yhteyden luomisen vaiheet

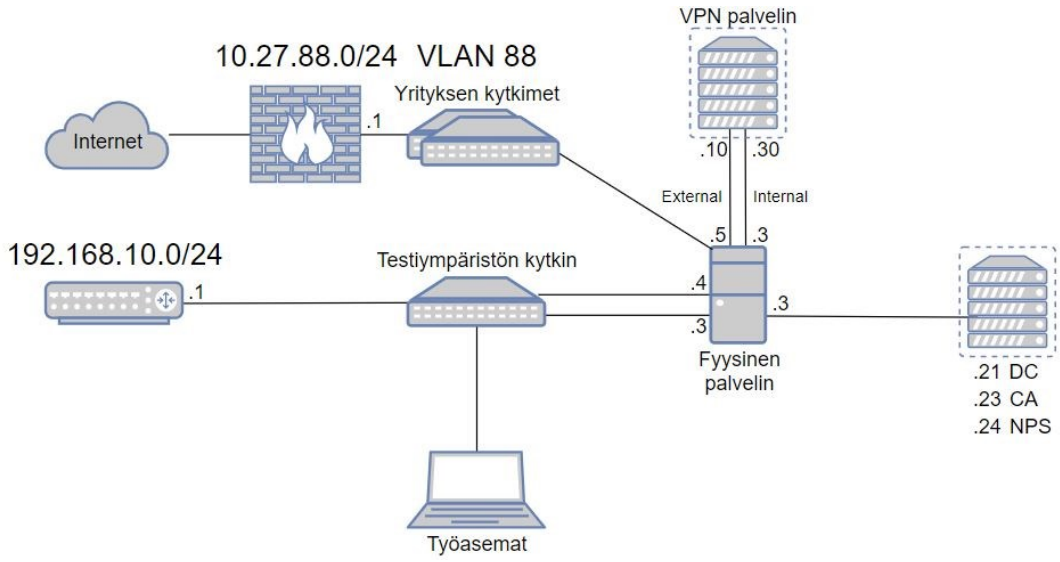
Vaiheet yhteyden luomisessa kertovat lyhyesti, kuinka etäyhteysratkaisu toimii ja mitä tehtäviä eri palvelimilla on (ks. Kuvio 8).

1. Yhteyden luominen alkaa, kun käyttäjä tekee nimiselvityksen VPN-palvelimen julkisesta osoitteesta.
2. Julkinen DNS palauttaa VPN-palvelimen osoitteen ja käyttäjä lähettää yhteys-pyynnön VPN-yhdyskäytävälle.
3. VPN-palvelimelle on kytketty RADIUS, jonka tarkoituksena on ohjata yhteys-pyyntö NPS-palvelimelle, joka tekee yhteyspyyntöjen käsittelyn.
4. NPS-palvelin käsittelee yhteyspyynnön, jonka lisäksi se suorittaa valtuutuksen sekä todennuksen suorittamisen, eli päättää yhteyspyynnön sallimisesta tai hylkäämisestä.
5. Access-Accept tai Access-Deny vastaus lähetetään NPS-palvelimelta VPN-palvelimelle.
6. Yhteys muodostetaan tai hylätään, riippuen NPS-palvelimen vastauksesta VPN-palvelimelle. (Always On VPN technology overview 2018.)

5 Etäyhteysratkaisun suunnittelu ja toteuttaminen

5.1 Lähtötilanne

Kokonaisuuden toteuttaminen lähti liikkeelle aiheeseen tutustumiselle ja siihen tarvittavien resurssien kartoittamisella. Tarvittavien palvelimien määrä, verkkolaitteet ja niiden tukemat protokollat selvitettiin. Jo heti alussa päätettiin, että ratkaisu toteutetaan erilliseen testiympäristöön (ks. Kuvio 9), johon tarvittaisiin Yritys X:n puolelta ainoastaan julkisen puolen osoite ja reititys palomuurilta testiympäristöön. Palvelinten osalta päädyttiin ratkaisuun, joka sisälsi yhden fyysisen palvelimen, johon otettiin käyttöön Hyper-V virtuaaliympäristö, jossa muut palvelimet toimivat. Fyysiseen palvelimeen lisättiin kaksi verkkoadapteria lisää, jotta yhteydet saadaan jaettua fyysiselle palvelimelle ja virtuaaliympäristön sisä- ja ulkoverkolle. Verkkolaitteiksi testiympäristön sisäverkolle otettiin käyttöön yksinkertainen 4G-reititin ja 24-porttinen kytkin kytkentöjä varten. Ulkoverkon toteutuksessa käytettiin Yritys X:n julkista IP-osoitetta, kahta kytkintä ja palomuuria. Palomuurille tehtiin reititys julkisesta osoitteesta sisäverkon osoiteavaruuteen, joka oli eri kuin testiympäristössä. Yritys X:n kytkimille määritettiin käyttöön Vlan 88, jotta testiympäristön lähiverkko voidaan pitää erillään yrityksen verkosta ja näin vaikuttaa myös turvallisuuteen.



Kuvio 9. Testiympäristön suunnittelu

Seuraavaksi aloitettiin palvelimien käyttöjärjestelmän kartoitus, jossa päädyttiin käyttämään Windows Server 2019 Standard, Desktop Experience käyttöjärjestelmiä. Valinta perustui tulevaisuuden näkökulmaan, sillä palvelimien päivitys uudempaan versioon voi olla tulevaisuudessa edessä. Tämän lisäksi haluttiin varmistaa, että ratkaisu toimii myös uudemmalla versiolla. Toinen vaihtoehto palvelinten käyttöjärjestelmäksi olisi ollut Windows Server 2016.

5.2 Testiympäristön käyttöönotto

Ennen Always On VPN toteutusta täytyi tehdä muutamia tarvittavia asennuksia ja määrityksiä infrastruktuurin pystyttämiselle. Varsinainen Always On VPN toteutus alkaa luvussa 5.3.

Testiympäristön toteuttaminen aloitettiin käyttöjärjestelmän asentamisella fyysiselle palvelimelle sekä 4G-reitittimen kevyellä konfiguroimisella, jossa otettiin DHCP pois käytöstä ja asetettiin default gateway osoite (ks. Kuvio 9). Fyysiselle palvelimelle asetettiin IP-osoite (ks. Taulukko 1) ja asennettiin Hyper-V rooli. Jotta verkot voidaan jakaa helposti, Hyper-V:n asetuksista täytyi luoda uusi virtuaalikytkin ja osoittaa se yhteen fyysisen koneen vapaista verkkoadaptereista. Uudelle sisäverkon virtuaalikytkimelle asetettiin IP-osoite (ks. Taulukko 1) ja tämän lisäksi virtuaalikytkin otettiin käyttöön jokaiselle virtuaalipalvelimella. Seuraavaksi aloitettiin virtuaaliympäristön pystyttäminen, jossa luotiin aluksi ”pohjakone”, josta muut virtuaalipalvelimet toteutettiin. Pohjakoneelle tehtiin päivitysten ja ohjelmien asennuksen jälkeen sysprep, joka mahdollistaa virtuaalikoneen kopioimisen/kloonaamisen, sillä sen avulla estetään mahdollisten identiteettiristiriitojen syntyminen. Tämän jälkeen pohjakoneesta kopiotiin tarvittava määrä palvelimia ja nimettiin ne.

Virtuaalipalvelimien osalta aloitettiin DC-palvelimesta, jolle asetettiin IP-osoite (ks. Taulukko 1) sekä asennettiin AD DS rooli. Palvelin määritettiin DC:ksi ja domain nimeksi määritettiin testiympäristöä varten keksitty ”aovlab.fi”. Tämän lisäksi palvelimelle asennettiin DNS, johon määritettiin reverse lookup zone käyttöön. Seuraavaksi asennettiin DHCP ja määritettiin työasemille DHCP scope 192.168.10.0, johon asetet-

tiin osoitteet 192.168.10.120 - 192.168.10.200. DHCP testattiin asettamalla ip-helper-address käyttöön testiympäristön kytkimelle, johon osoitettiin DC-palvelimen IP-osoite. Kytkimeen liitetty työasema sai osoitteet oikeasta osoiteavaruudesta.

Seuraavaksi siirryttiin CA-palvelimen asennukseen, jolle asetettiin IP-osoite (ks. Taulukko 1), asennettiin AD CS ja tehtiin tarvittavat konfiguroinnit, jotta testiympäristön PKI saadaan pystytettyä. CA nimeksi määritettiin aovlab-CA.

NPS-palvelimelle ja VPN-palvelimelle asetettiin tässä vaiheessa ainoastaan IP-osoitteet (ks. Taulukko 1). Kaikki virtuaalikoneet nostettiin asennusten ja määritysten lisäksi testiympäristön toimialueeseen (aovlab.fi).

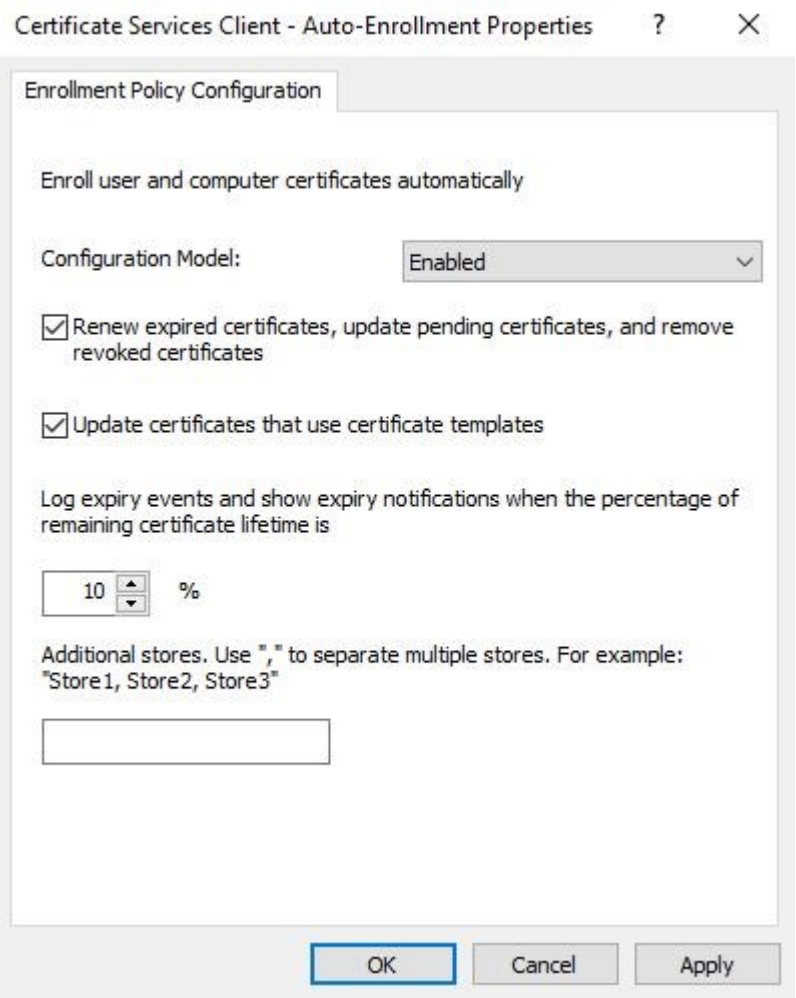
Taulukko 1. Palvelimien IP-osoitteet

Palvelimen nimi	Verkkoadapteri	IP-osoite	Default Gateway
Fyysinen palvelin	External Hyper-V Internal Hyper-V External	192.168.10.4 192.168.10.3 10.27.88.5	192.168.10.1 192.168.10.1 10.27.88.1
DC1.aovlab.fi	Hyper-V Internal	192.168.10.21	192.168.10.1
CA1.aovlab.fi	Hyper-V Internal	192.168.10.23	192.168.10.1
NPS1.aovlab.fi	Hyper-V Internal	192.168.10.24	192.168.10.1
VPN1.aovlab.fi	Hyper-V Internal Hyper-V External	192.168.10.30 10.27.88.10	192.168.10.1 10.27.88.1

5.3 Always On VPN -etäyhteysratkaisun käyttöönotto

Kun testiympäristön infrastruktuuri oli saatu valmiiksi, siirryttiin konfiguroimaan Always On VPN ratkaisun käyttöönottoon tarvittavia asioita. Käyttöönotossa hyödynnettiin Microsoftin tarjoamaa ohjetta (Deploy Always On VPN 2018).

Konfigurointi aloitettiin DC-palvelimelta, johon määritettiin aluksi käyttöön sertifikaattien automaattinen lisäys GPO:n avulla. Tämä tehtiin luomalla aluksi uusi GPO ja muokkaamalla sen **Sertificate Services Client – Auto-Enrollment** asetuksia (ks. Kuvio 10). Kyseinen määritys tehtiin käyttäjien ja tietokoneiden **Sertificate Services Client – Auto-Enrollment** asetuksiin. VPN-yhteyden todennus suoritetaan sertifikaattien avulla, joten toimenpide liittyy käyttäjien todennuksen automatisointiin.



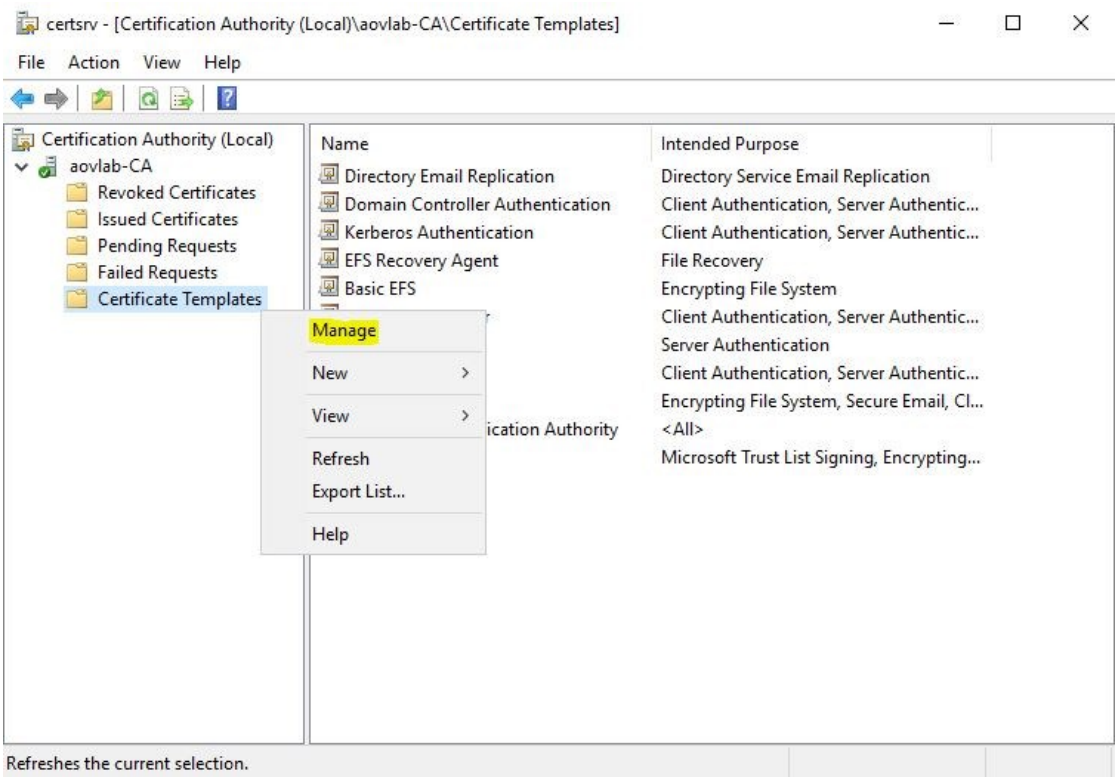
Kuvio 10. Auto-Enrollment Properties

Seuraavaksi DC-palvelimelle tehtiin ryhmät VPN-käyttäjille, VPN-palvelimille ja NPS-palvelimille. Selkeyden vuoksi luotiin **Ryhmät** OU, johon kyseiset ryhmät sijoitettiin. Ryhmiin lisättiin jäseniksi asiaankuuluvat käyttäjät tai koneet (ks. Taulukko 2).

Taulukko 2. Ryhmät

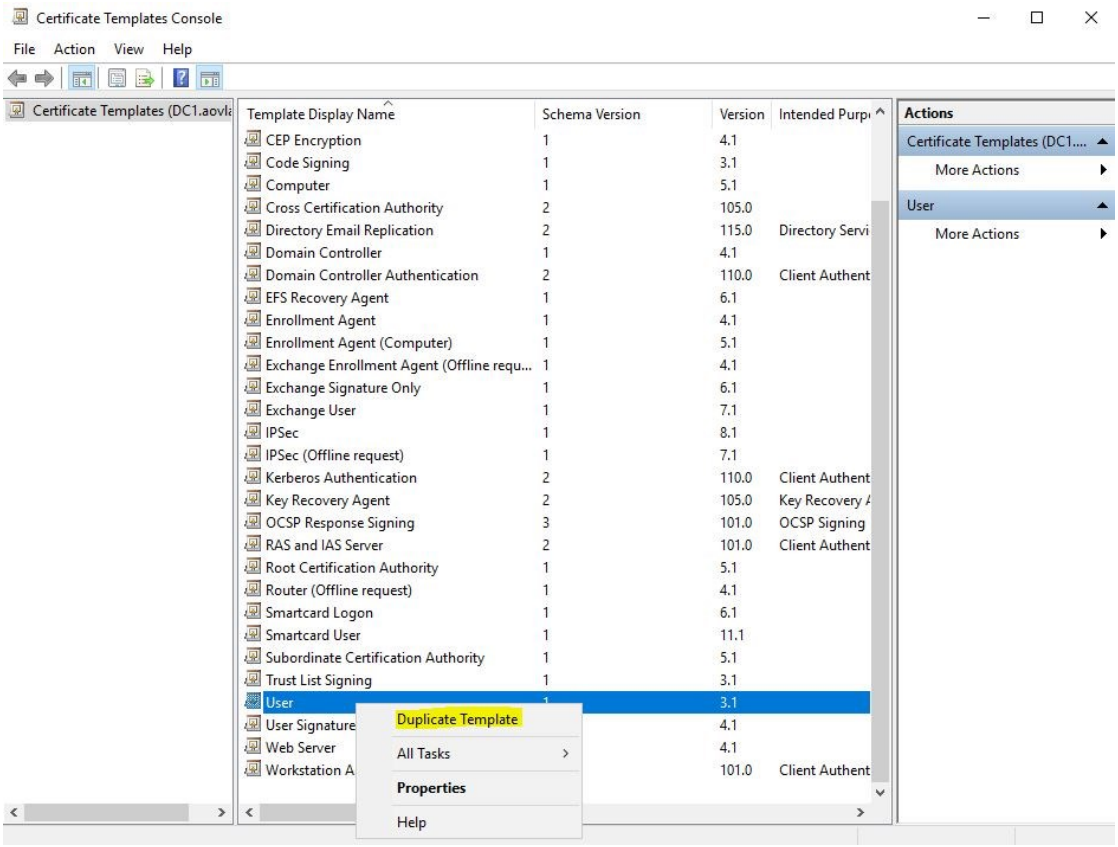
Ryhmä	Käyttäjä/kone
VPN Users	Teppo Testaaja
VPN Servers	VPN1
NPS Servers	NPS1

Tässä vaiheessa siirryttiin CA-palvelimelle tekemään mukautettu todennusmalli asiakkaan ja palvelinten todentamista varten, jonka tarkoituksena on parantaa varmenteiden yleistä tietoturvaa. Todennusmallin luominen aloitettiin avaamalla **Certification Authority** palvelimen hallinnasta ja menemällä varmennepohjien hallintaan (ks. Kuvio 11).



Kuvio 11. Certificate Templates

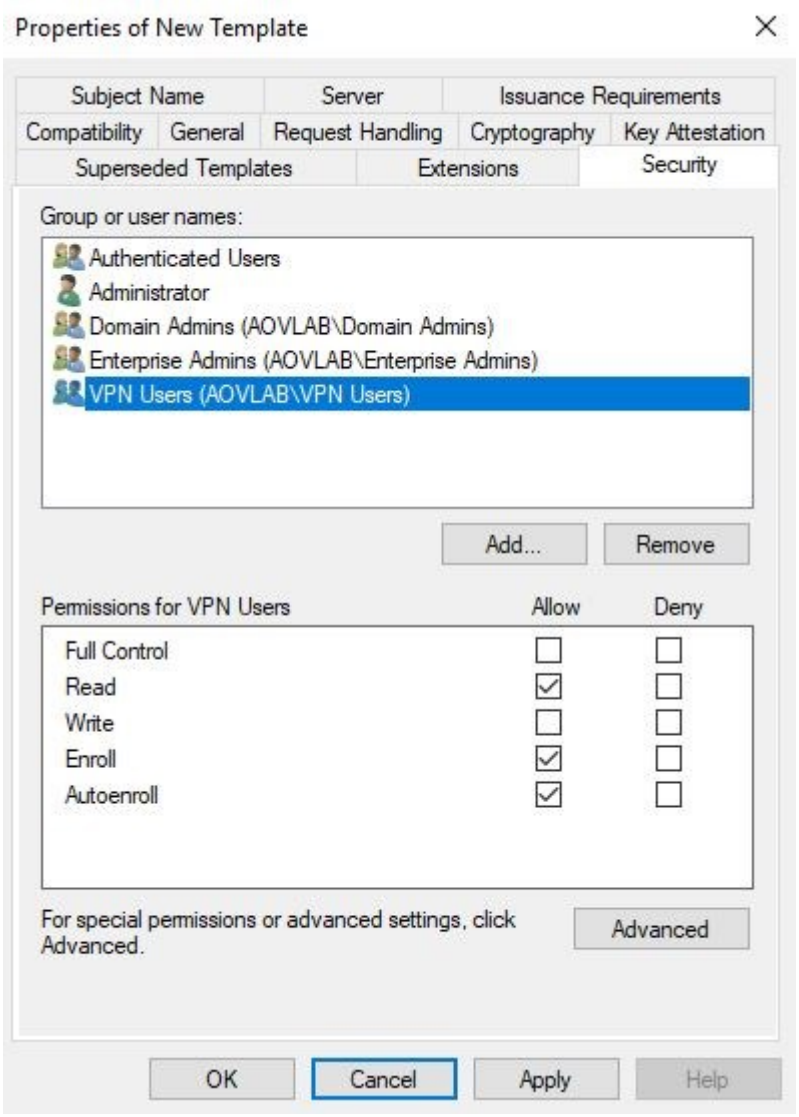
Seuraavaksi avautuvasta hallintapaneelissa etsittiin listalta käyttäjäpohja (user template) ja tehtiin siitä kaksoiskappale (ks. Kuvio 12). Uuden varmennepohjan luomisessa huomioitavaa on, että kaikki tarvittavat määritykset on tehtävä loppuun ennen ”OK” tai ”Apply” painikkeiden painamista, sillä useita asetuksia ei pääse enää jälkeenpäin muokkaamaan. Pohja täytyy luoda uudestaan useassa tapauksessa, jos määrityksiä pitää muokata jälkeenpäin.



Kuvio 12. Duplicate template

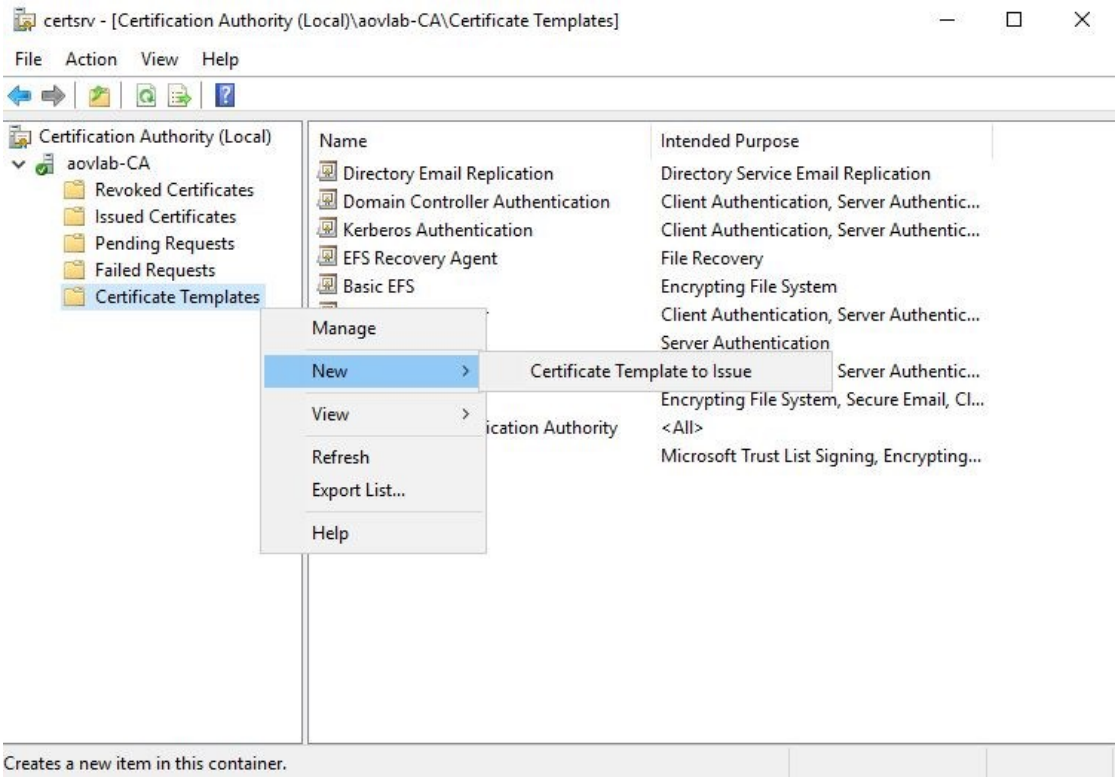
Uuden pohjan asetuksien määritys aloitettiin **General** välilehdeltä, johon vaihdettiin pohjan nimi viittaamaan käyttäjän todentamista, eli **VPN User Authentication**. Tämän lisäksi poistettiin valinta, joka jakaa sertifikaatin AD:ssa. **Security** välilehdellä lisättiin aiemmin luotu **VPN Users** ryhmä ja annettiin ryhmälle oikeudet sertifikaattien automaattista jakoa varten (ks. Kuvio 13). Ryhmistä poistettiin tämän lisäksi **Domain Users** ryhmä, sillä sertifikaatteja ei haluta jakaa kaikille toimialueen käyttäjille. **Compatibility** välilehdelle määritettiin yhteensopivuusasetukset, jotka määrittelevät

mistä palvelimen tai tietokoneen käyttöjärjestelmistä asti olevat sertifikaatit ovat yhteensopivia. Koska tämä ei näennäisesti vaikuta toimivuuteen, valittiin **Windows Server 2012 R2** ja **Windows 8.1**. **Request Handling** välilehdeltä poistettiin valinta, joka mahdollistaisi yksityisen avaimen viemisen. **Cryptography** välilehdellä kategoriaksi valittiin **Key Storage Provider** ja toimittajaksi **Microsoft Platform Crypto Provider**, jonka avulla sertifikaatin toimittamisen tietoturvaa parannetaan. **Subject Name** välilehdellä poistettiin valinnat sähköpostia koskevista kohdista, sillä testiympäristössä sähköposteja ei ole listattu käyttäjille.



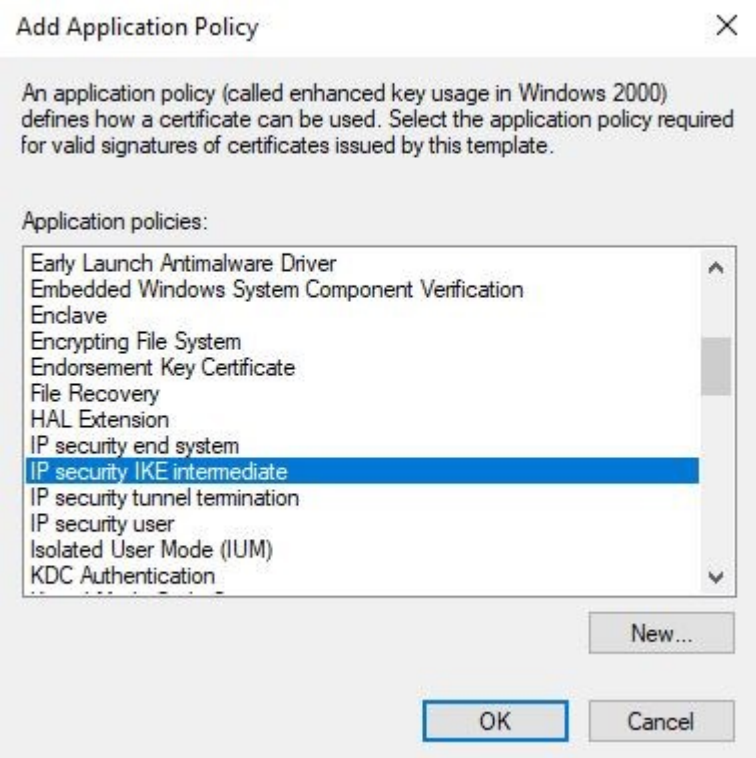
Kuvio 13. New template security

Lopuksi hyväksyttiin tehdyt määritykset ja suljettiin hallintapaneeli. Tämän jälkeen luotu pohja käytiin ottamassa käyttöön valitsemalla **Certificate Template to Issue** valinta **Certificate Templates** kohdasta (ks. Kuvio 14). Avautuvalta listalta etsittiin luodun pohjan nimi, eli **VPN User Authentication** ja otettiin se käyttöön.



Kuvio 14. Certificate Template to Issue

VPN-palvelin tarvitsee myös todennuspohjan, joten sen määrittäminen aloitettiin seuraavaksi. Pohjan tekeminen aloitettiin samalla tavalla kuin käyttäjäpohjan, eli siirryttiin aluksi sertifikaattipohjien hallintapaneeliin (ks. Kuvio 11) ja tämän jälkeen listalta etsittiin **RAS and IAS Server**, josta tehtiin kaksoiskappale. **General** välilehdelle tehtiin ainoastaan uuden pohjan nimeäminen. Tämän jälkeen **Extensions** välilehdellä lisätään **IP security IKE intermediate** käytäntö sovelluskäytäntöihin, sillä sen avulla mahdollistetaan varmenteiden suodatus (ks. Kuvio 15). Tämä tarkoittaa, että jos VPN-palvelimella on useampia todennukseen käytettäviä sertifikaatteja, IPSec käyttää sertifikaattia, jossa on molemmat EKU-vaihtoehdot. Tämä on myös tärkeä osa IKEv2-todennusta, sillä ilman kyseistä käytäntöä todennus voi epäonnistua.

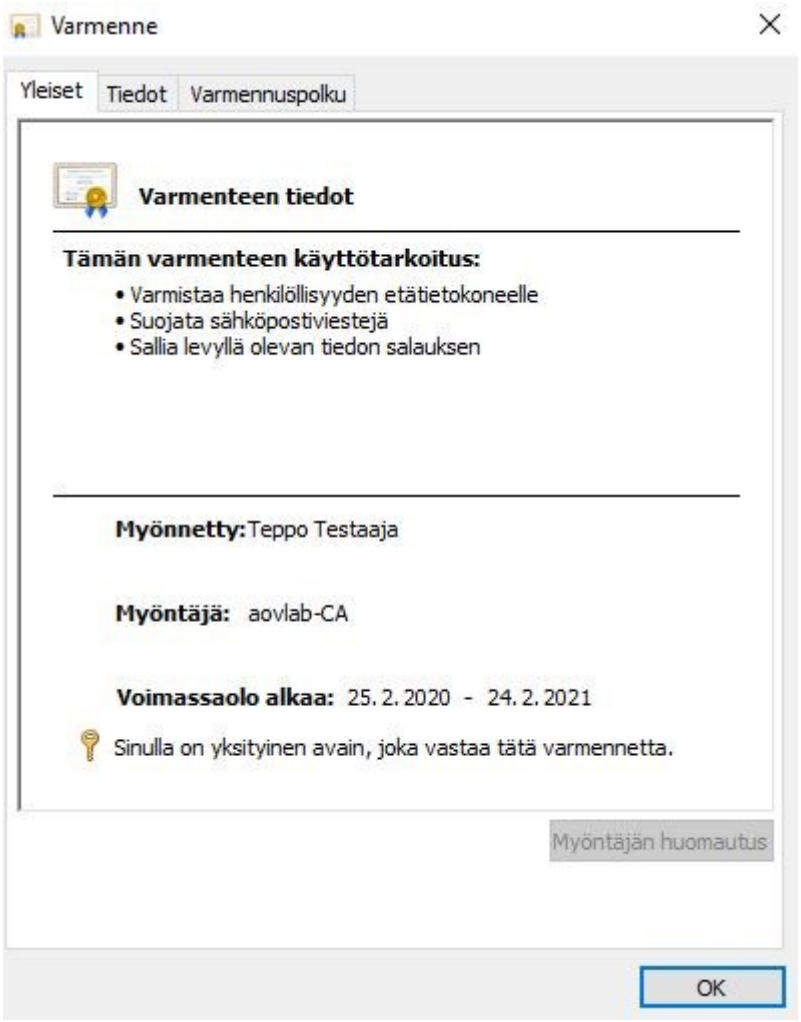


Kuvio 15. IP security IKE intermediate

Tämän jälkeen siirryttiin **Security** välilehdelle, jossa tehtiin samantyylisiä asioita, kuin käyttäjän pohjan kanssa, eli lisättiin **VPN Servers** ryhmä, jolle sallittiin **Enroll**. Tämän lisäksi ryhmistä poistettiin **RAS and IAS Servers** ryhmä. **Subject Name** välilehdellä määritettiin **Supply in the request**, sillä sertifikaattia ei jaeta automaattisesti. **Request Handling** välilehdellä voitaisiin määritellä **Allow private key to be exported** käyttöön, jos osaksi kokonaisuutta oltaisiin ottamassa conditional access sääntöjä, mutta koska testiympäristön toteutuksessa tätä ei tehdä, jätettiin valinta tyhjäksi. Pohja oli näiden toimenpiteiden jälkeen valmis ja muutokset hyväksyttiin. Tämän jälkeen pohja otettiin käyttöön samalla tavalla kuin käyttäjän pohja (ks. Kuvio 14), jossa listalta etsittiin **General** välilehdelle määritetty nimi.

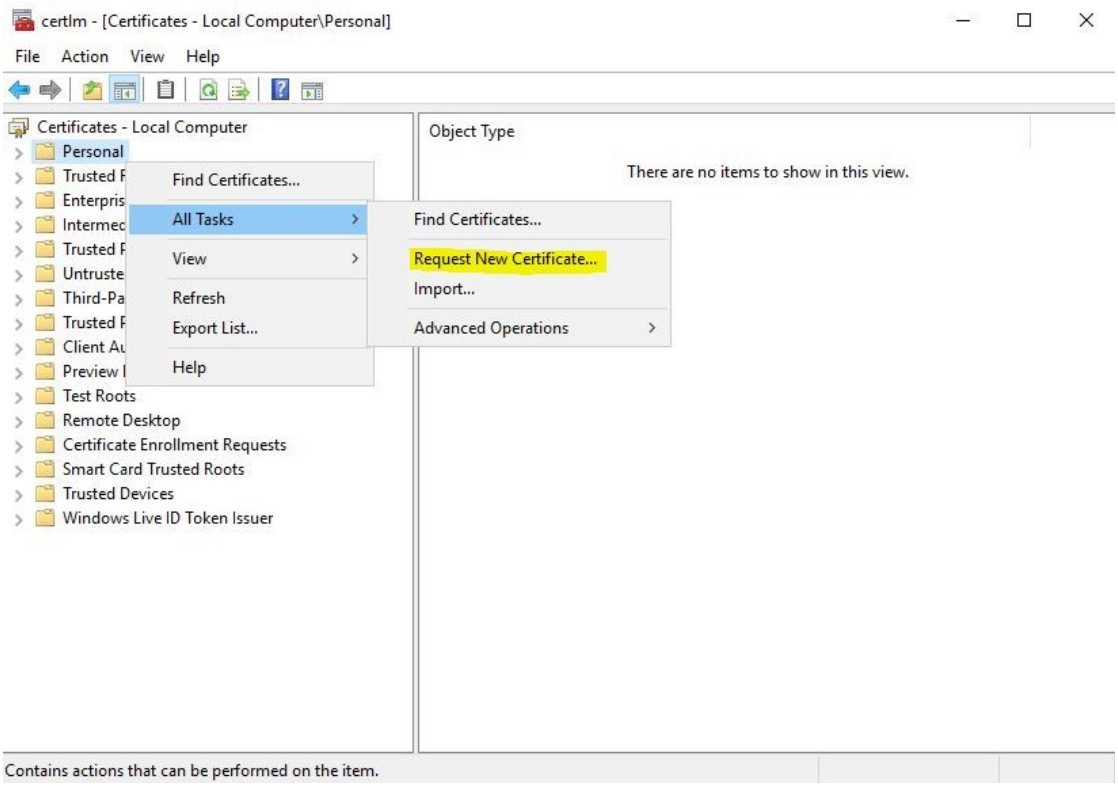
Viimeiseksi tehtiin NPS-palvelimen pohja, joka toteutettiin samalla tavalla kuin VPN-palvelimen pohja. Eroina näillä pohjilla oli **General** välilehdelle määritetty nimi, **Extensions** välilehdellä ei tehty muutoksia ja **Security** välilehdelle määritettiin **NPS Servers** ryhmä ja sallittiin **Enroll** ja **Autoenroll**. Lopuksi pohja otettiin käyttöön samallatavalla, kuin aiemmatkin (ks. Kuvio 14), mutta käyttäen **General** välilehdelle määritettyä nimeä.

Tässä vaiheessa varmistettiin käyttäjien ja palvelimien sertifikaattien ilmoittautuminen, joka aloitettiin käyttäjän sertifikaatista. Toimialueeseen liitetylle testikoneelle kirjauduttiin **VPN Users** ryhmään kuuluvalla käyttäjällä (ks. Taulukko 2) sekä päivitettiin group policy *gpupdate /force* – komennolla. Tämän jälkeen avattiin käyttäjän henkilökohtaiset sertifikaatit, josta käyttäjälle myönnetty sertifikaatti löytyi (ks. Kuvio 16).



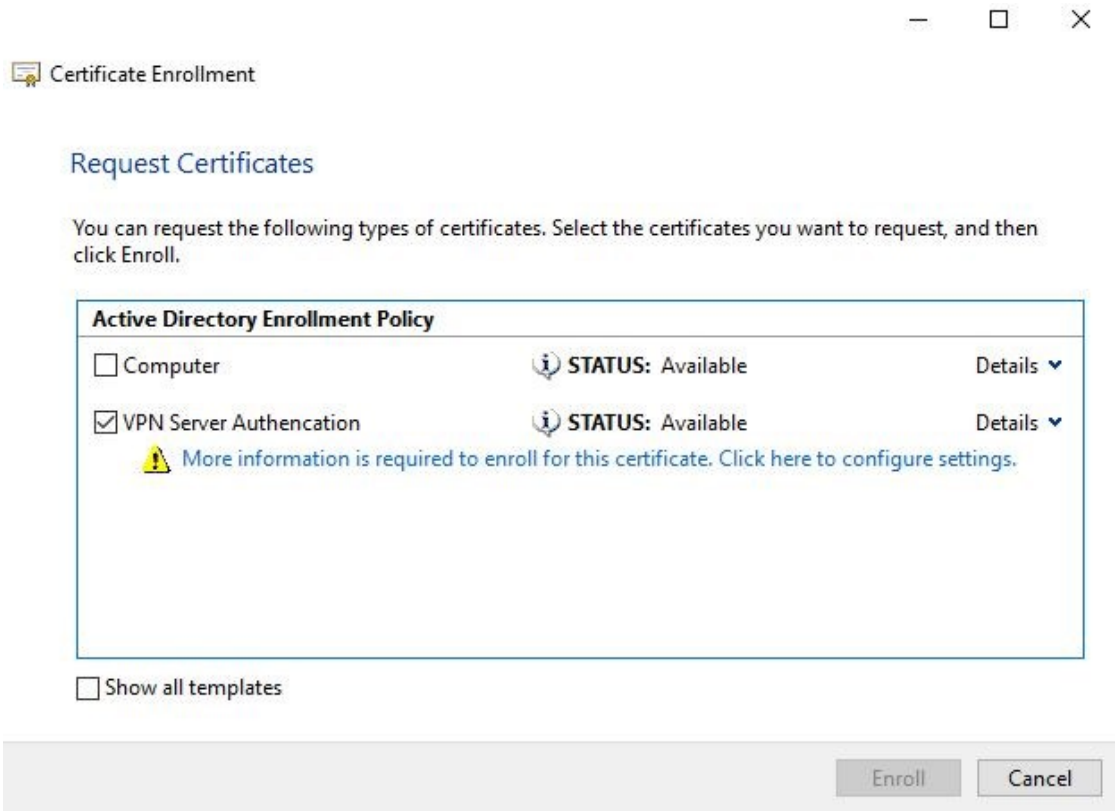
Kuvio 16. Käyttäjän sertifikaatti

VPN-palvelimen sertifikaattia ei jaeta automaattisesti, joten sen kohdalla se täytyi pyytää manuaalisesti. Tämä onnistui menemällä sertifikaattienhallintaan (certlm.msc) ja tekemällä pyyntö sieltä (ks. Kuvio 17).



Kuvio 17. Request New Certificate

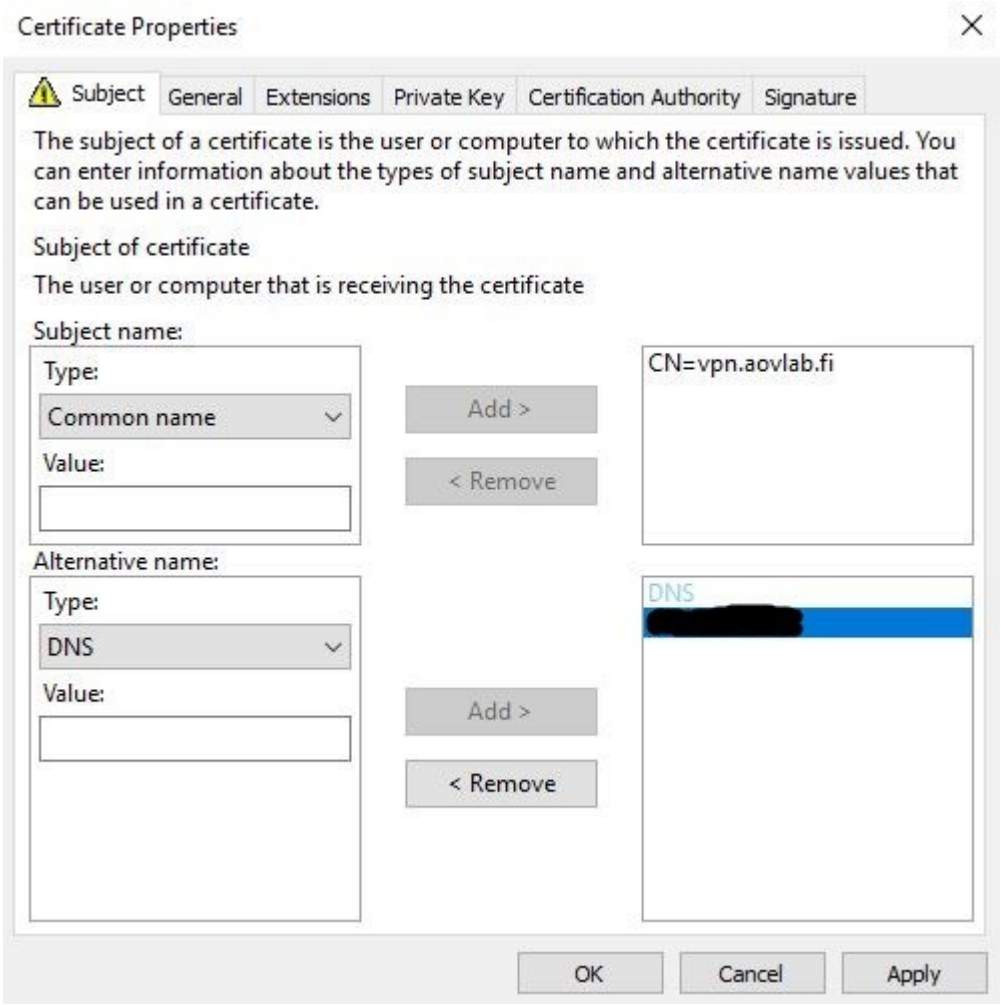
Sertifikaattien pyyntövaiheessa tulisi näkyä aiemmin luotu pohja VPN-palvelimien todentamiseen, jonka asetuksiin täytyy tehdä muutoksia ennen varsinaista sertifikaatin pyytämistä painamalla nimen alla näkyvää linkkiä (ks. Kuvio 18). Ennen tätä DC-palvelimelle tehtiin alias VPN-palvelimen nimestä DNS:n asetuksiin (ks. Kuvio 19), sillä yksityistä nimeä käytetään määrityksissä.



Kuvio 18. Request Certificates

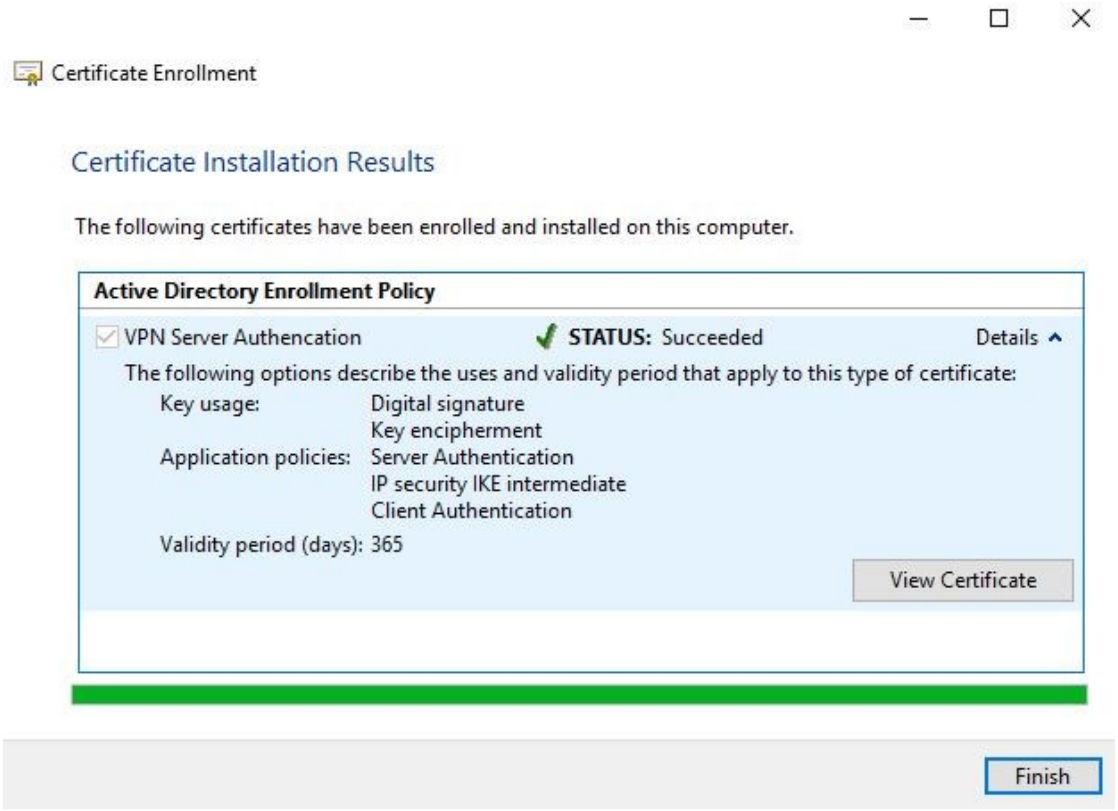
Kuvio 19. DNS Alias (CNAME)

Seuraavaksi muokataan sertifikaatin määrityksiä (ks. Kuvio 20). **Subject Name** kentän **Type** alasvetovalikosta valittiin **Common name** ja sen alapuolella olevaan kenttään syötettiin DNS aliaksen nimi (ks. Kuvio 19). **Alternative name** kentän **Type** alasvetovalikosta valittiin **DNS** ja alapuolella olevaan kenttään syötettiin julkinen IP-osoite, josta VPN-palvelin löytyy. Julkinen IP-osoite on piilotettu kuvasta. Tämä tehtiin, koska julkiselle osoitteelle ei testiympäristön takia määritetty julkista DNS-nimeä, mutta tämä on suositeltavaa tuotantoympäristön toteutuksissa. Tehdyt valinnat lisättiin molemmista kentistä **Add** painikkeella. Lopuksi määritykset hyväksyttiin OK painikkeella.



Kuvio 20. Certificate Properties

Kun sertifikaatin pyyntö on tehty onnistuneesti, varmistetaan että sertifikaatin tiedoista löytyy aiemmin määritetty **IP security IKE intermediate** (ks. Kuvio 21).



Kuvio 21. Certificate Installation Results

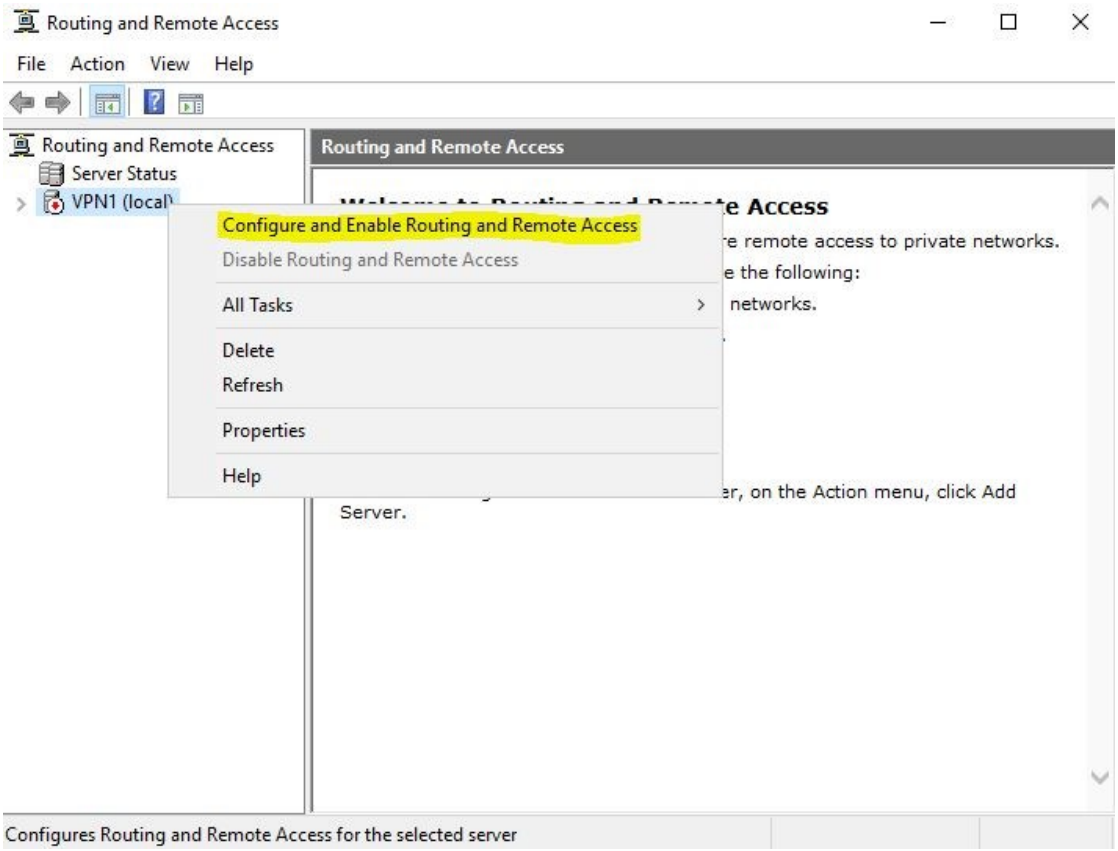
NPS-palvelimen sertifikaatti tulee käyttäjien tavoin automaattisesti ja tämän takia sen löytyminen täytyi ainoastaan varmistaa (ks. Kuvio 22). Sertifikaatit löytyvät lokaaleista sertifikaateista, joita pääsee tarkastelemaan sertfikaattien hallintapaneeli.

Kuvio 22. NPS-palvelimen sertifikaatti

5.3.1 VPN-palvelimen konfigurointi

VPN-palvelin tarvitsee toimiakseen oikein kaksi verkkoadapteria, toinen sisäverkkoon ja toinen ulkoverkkoon. Tämän takia fyysisen palvelimen Hyper-V asetuksissa luotiin uusi virtuaalikytkin ja lisättiin sen VPN-palvelimelle. Uusi virtuaalikytkin osoitti siis yhteen fyysisen palvelimen vapaista verkkoadaptereista. Kyseinen adapteri kytkettiin fyysisesti Yritys X:n kytkimeen. Fyysisen palvelimen uudelle virtuaaliadapterille (Hyper-V External) asetettiin IP-osoite, jonka jälkeen VPN-palvelimella asetettiin uuteen verkkoadapteriin IP-osoite samasta osoiteavaruudesta (ks. Taulukko 1). Palomuurin asetukset julkisesta osoitteesta kyseiseen lähiverkkoon on esitetty luvussa 5.3.3. Tämän lisäksi VPN-palvelimelle täytyi avata portteja palvelimen omasta palomuurista IKEv2 ja RADIUS toimintoja varten. Portit saapuvan liikenteen osalta olivat UDP 500 ja UDP 4500, jotka koskivat IKEv2:ta. Lähtevän liikenteen osalta avattiin UDP 1812 portti RADIUS:ta varten, eli liikenne VPN-palvelimelta NPS-palvelimelle.

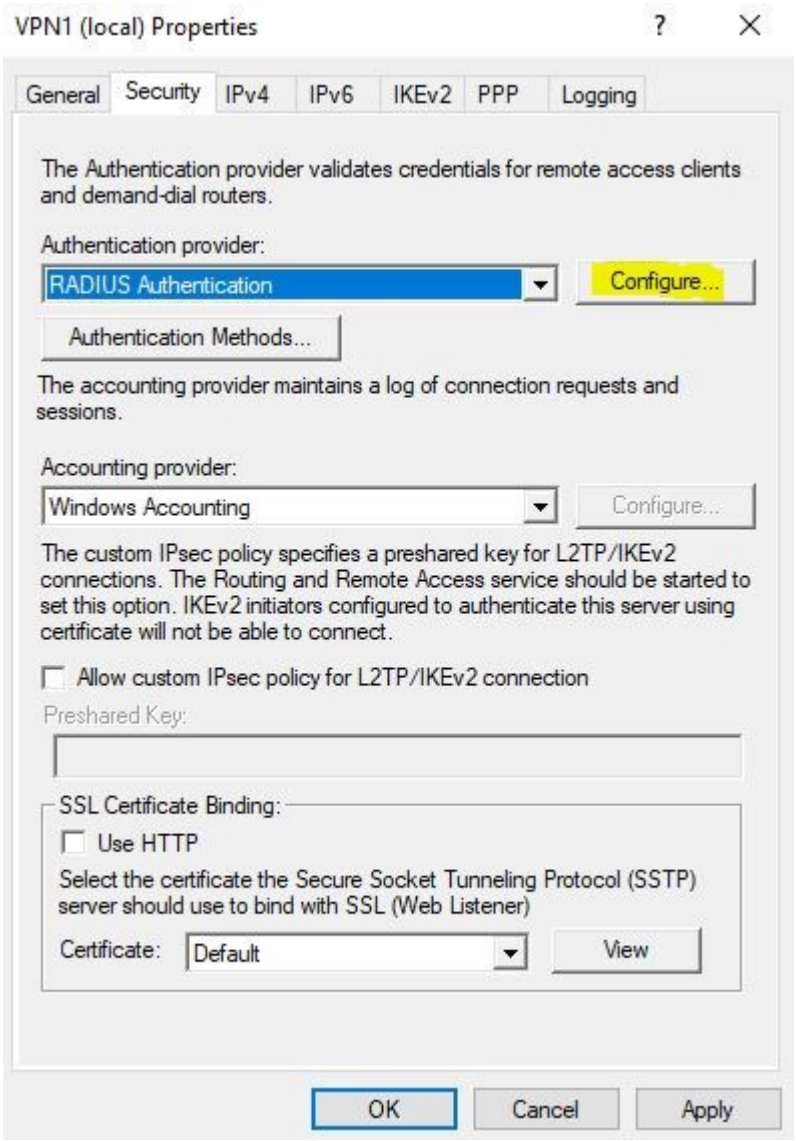
Asennukset ja niiden määritykset aloitettiin asentamalla **Remote Access** ja määrittämällä sen rooliksi **Direct Access and VPN (RAS)**. Asennuksen jälkeen päätettiin, mikä etäyhteys tapa otetaan käyttöön. Tähän valittiin **Deploy VPN only**, sillä käyttöön haluttiin ottaa RRAS, ei Direct Access toimintoja. Tämän jälkeen avautuvasta **Routing and Remote Access** ikkunasta aloitettiin RRAS konfigurointi ja sen käyttöönotto (ks. Kuvio 23).



Kuvio 23. Configure and Enable RRAS

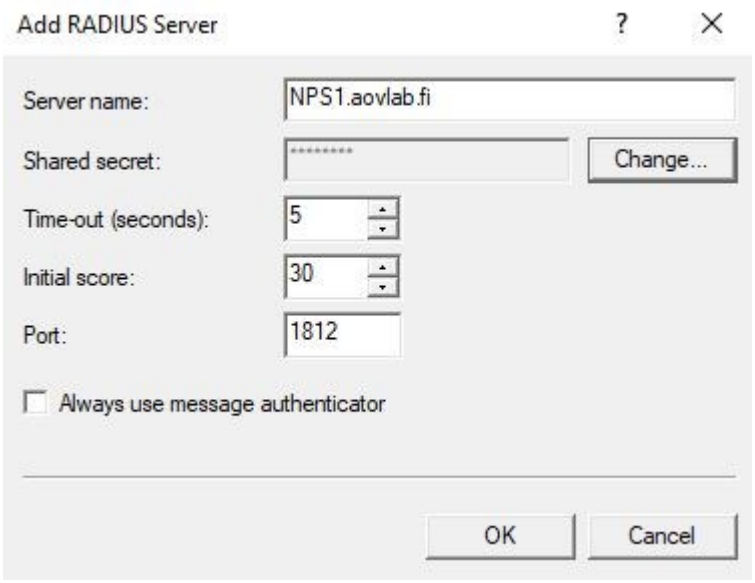
Käyttöönoton **Configuration** vaiheessa valitaan **Custom Configuration**, jotta seuraavasta ikkunasta voidaan valita ainoastaan **VPN access**. Tämän jälkeen palvelu pystyttiin käynnistämään ruudulle ilmestyneestä **Start service** painikkeesta.

Kun palvelu saatiin käynnistettyä, päästiin sen asetuksiin tekemään tarvittavia muutoksia, joiden avulla IKEv2 yhteydet sallittiin ja IP-osoitteet etäyhteyden käyttäjille saatiin määritettyä. Asetuksia päästiin muokkaamaan RRAS hallintapaneelissa valitsemalla palvelimen nimestä hiiren oikealla painikkeella ja tämän jälkeen valitsemalla **Properties**. Avautuneessa ikkunassa siirryttiin aluksi **Security** välilehdelle, jossa määritettiin todennuksen tarjoaja ja sen konfigurointi (ks. Kuvio 24).



Kuvio 24. RRAS Authentication provider

Seuraavaksi tehtiin RADIUS-palvelimen määritykset (ks. Kuvio 25), joihin tässä tapauksessa määritettiin NPS-palvelin, joka toimii RADIUS-palvelimena. Tämän lisäksi luotiin uusi **Shared secret** salasana, joka otettiin talteen, sillä sitä tarvittiin myöhemmin NPS-palvelimen määrityksissä.



Kuvio 25. RADIUS-palvelimen lisäys

Tämän jälkeen määritettiin IP-osoitteet etäyhteyden käyttäjille siirtymällä **IPv4** välilehdelle, johon luotiin uusi staattinen osoiteavaruus. Osoitteiksi määritettiin 192.168.10.200 – 192.168.10.220. Tuotantoympäristöön tulee ehdottomasti määrittää enemmän osoitteita, mutta se ei ollut olennaista testiympäristön toteutuksessa. DHCP on myös mahdollista ottaa käyttöön, mutta se ei ole pakollista.

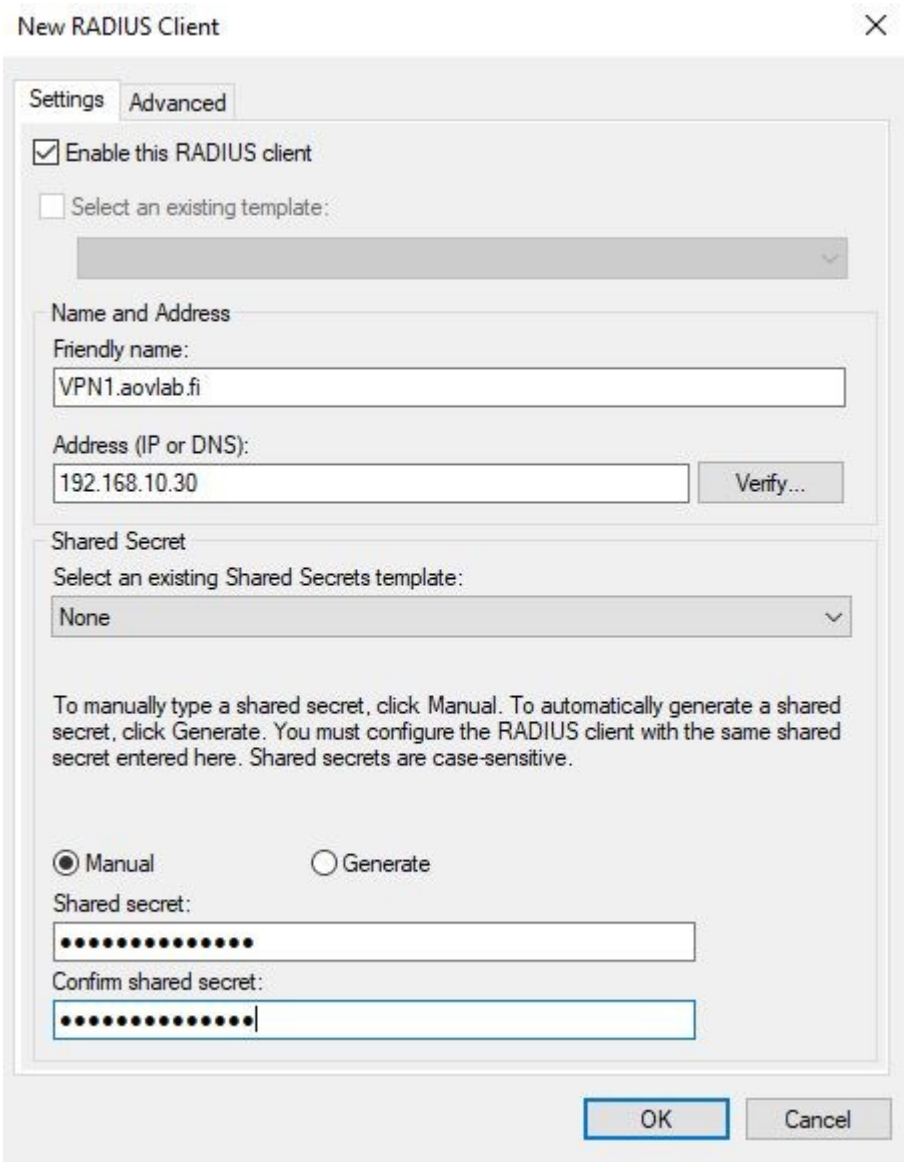
Jos käyttöön otettaisiin conditional access sääntöjä, tulisi **Security** välilehdeltä ottaa käyttöön VPN-palvelimen todennus valitsemalla alhaalta **SSL Certificate Binding** asetuksien **Certificate** alasvetovalikosta VPN-palvelimen todennus. Tätä ei kuitenkaan oteta testiympäristössä käyttöön, joten se jätettiin valitsematta.

Portteihin tehtiin myös muutoksia, joilla pystyttiin vaikuttamaan muun muassa mitä portteja käytetään ja montako samanaikaista VPN-yhteyttä tuetaan. Porttien asetuksia päästiin muokkaamaan RRAS hallintapaneelista, valitsemalla **Ports** hiiren oikealla painikkeella ja tämän jälkeen valitsemalla **Properties**. Porttien asetuksista otettiin **WAN Miniport (SSTP)** pois käytöstä, sillä kyseisiä portteja ei haluta käytettävän. Muut porteista jätettiin oletusasetuksille. Porttien asetuksissa **Maximum ports** kohta kertoo tuettujen samanaikaisten VPN-yhteyksien määrän, joka on oletuksena 128.

5.3.2 NPS-palvelimen konfigurointi

NPS-palvelimen tehtävänä on varmistaa, että käyttäjällä on lupa muodostaa yhteys ja samalla suorittaa käyttäjän todentaminen. Se kuuntelee RADIUS-liikennettä portissa 1812, jonka avaus tapahtuu automaattisesti asennuksen yhteydessä.

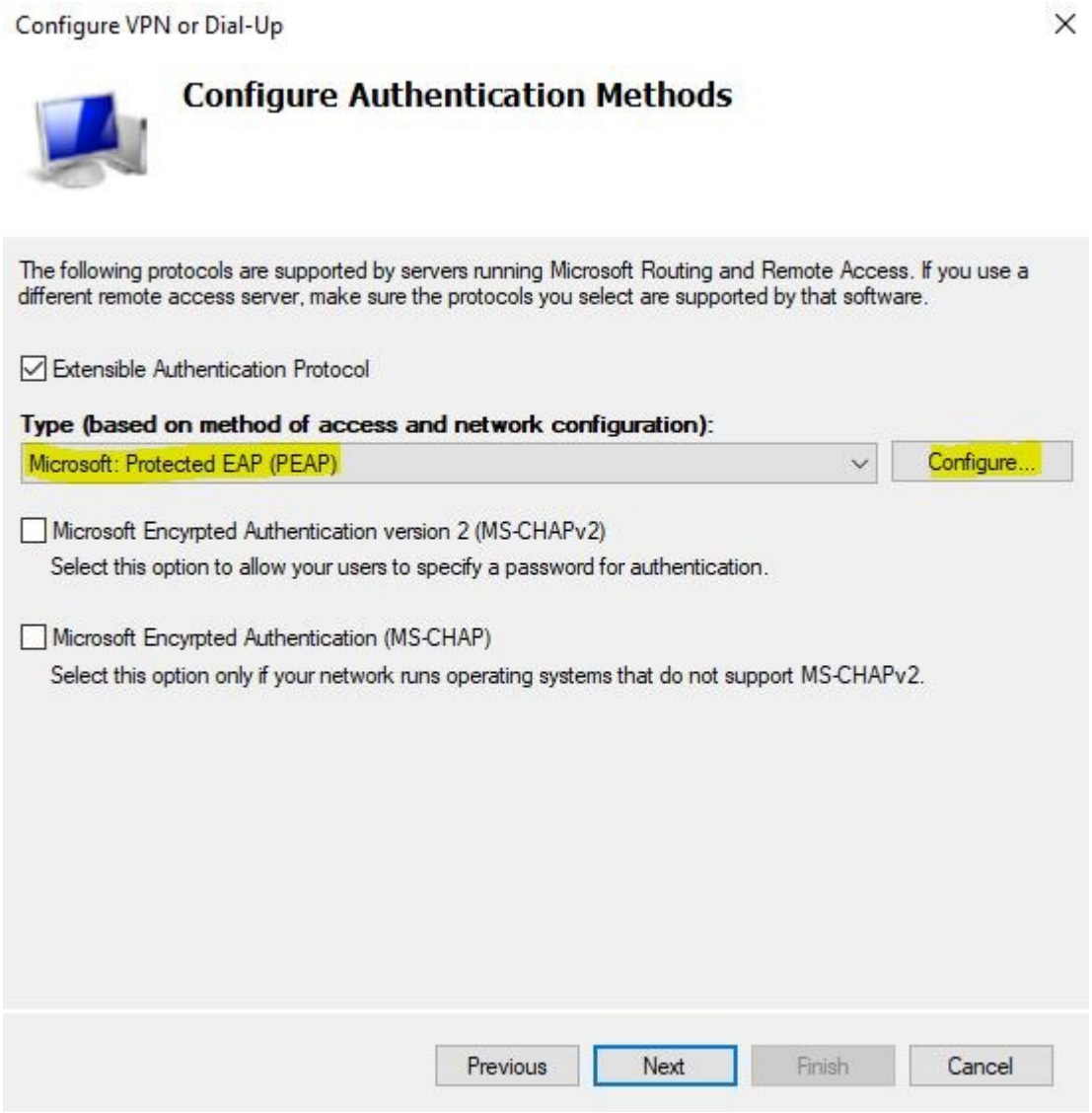
NPS-palvelimen konfigurointi aloitettiin asentamalla **Network Policy and Access Services** rooli palvelimen hallinnasta. Palvelin rekisteröitiin Active Directoryyn, jotta sillä on oikeudet päästä tarkastamaan käyttäjätietoja ja käsitellä yhteyspyyntöjä. Tämä tehtiin avaamalla **Network Policy Server** ja valitsemalla **NPS (Local)** hiiren oikealla ja tämän jälkeen valitsemalla **Register server in Active Directory**. Seuraavaksi aloitettiin VPN-palvelimen lisääminen RADIUS asiakkaaksi, joka tehtiin listalla olevasta **RADIUS Clients and Servers** kohdasta ja tämän jälkeen valitsemalla aluksi hiiren vasemmalla painikkeella **RADIUS Clients** kohdasta ja tämän jälkeen valitsemalla **New**. Uuden RADIUS asiakkaan (ks. Kuvio 26) tietoihin syötetään sopiva nimi, esimerkiksi palvelimen nimi, osoite tai FQDN, joka suositellaan vielä varmistettavan **Verify** painikkeella, jotta varmistetaan että uusi RADIUS asiakas on tavoitettavissa kyseistä osoitteesta/FQDN. Lopuksi alas syötettiin aiemmin määritetty **Shared secret**, joka lisättiin VPN-palvelimella (ks. Kuvio 25). Kun kaikki määritykset on tehty, hyväksytään uuden RADIUS asiakkaan luominen.



Kuvio 26. Uusi RADIUS-asiakas

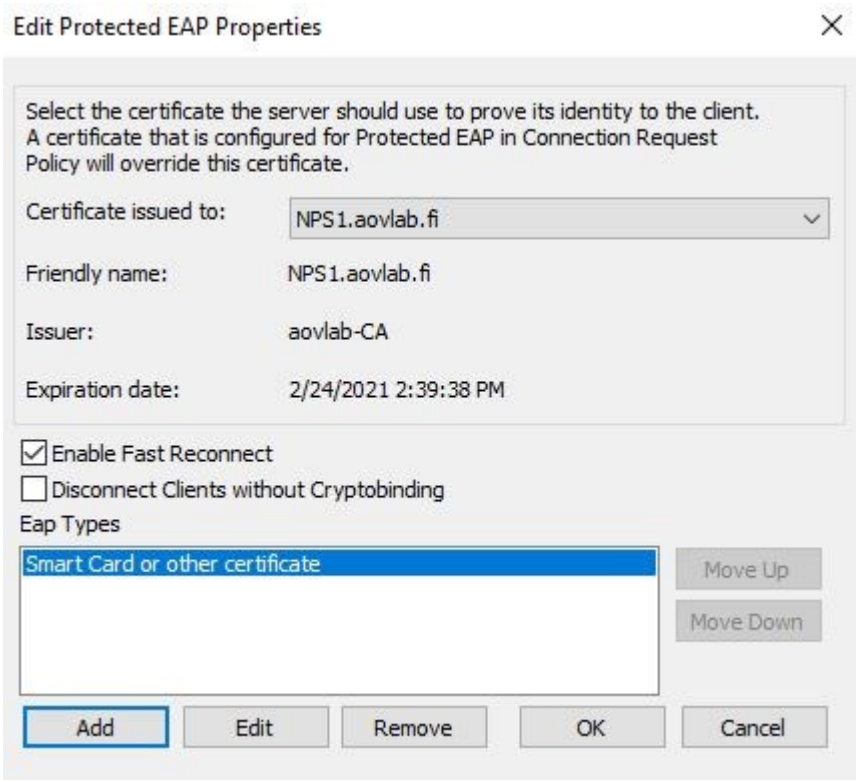
Tämän jälkeen määritettiin NPS-palvelin RADIUS-palvelimeksi, joka aloitettiin menemällä **Network Policy Server** hallintapaneelissa **NPS (Local)** kohtaan ja valitsemalla oikealla näkyvästä ikkunasta **Configure VPN or Dial-Up** painike. Huomioitavaa on, että tämän painikkeen yläpuolella olevassa alasvetovalikossa tulisi olla valittuna **RADIUS server for Dial-Up or VPN Connections** valinta. Seuraavaksi avautuvasta ikkunasta valittiin **Virtual Private Network (VPN) Connections**, koska oltiin määrittämässä VPN-yhteyksiä. Tämän jälkeen lisättiin äsken luotu RADIUS asiakas, jonka nimi vastaa **Friendly name** kenttään asetettua nimeä (ks. Kuvio 26). Seuraavaksi määritettiin käytettävät todennustavat (ks. Kuvio 27), johon valittiin **Extensible Authentication Protocol** ja alasvetovalikosta **Microsoft: Protected EAP (PEAP)**. Muut valinnat

poistettiin. Ennen jatkamista tehtiin vielä muutoksia PEAP konfiguraatioon **Configure** painikkeesta.



Kuvio 27. Authentication Methods

PEAP määrityksien tarkoituksena on valita käytettävät todennustavat, sekä kertoa mitä sertifikaattia käytetään palvelimen todentamiseen. Kyseisessä toteutuksessa käytettiin siis NPS-palvelimen sertifikaattia ja todennustavaksi valittiin ainoastaan **Smart Card or other certificate**, jonka avulla todennus voidaan suorittaa sertifikaattien avulla (ks. Kuvio 28).



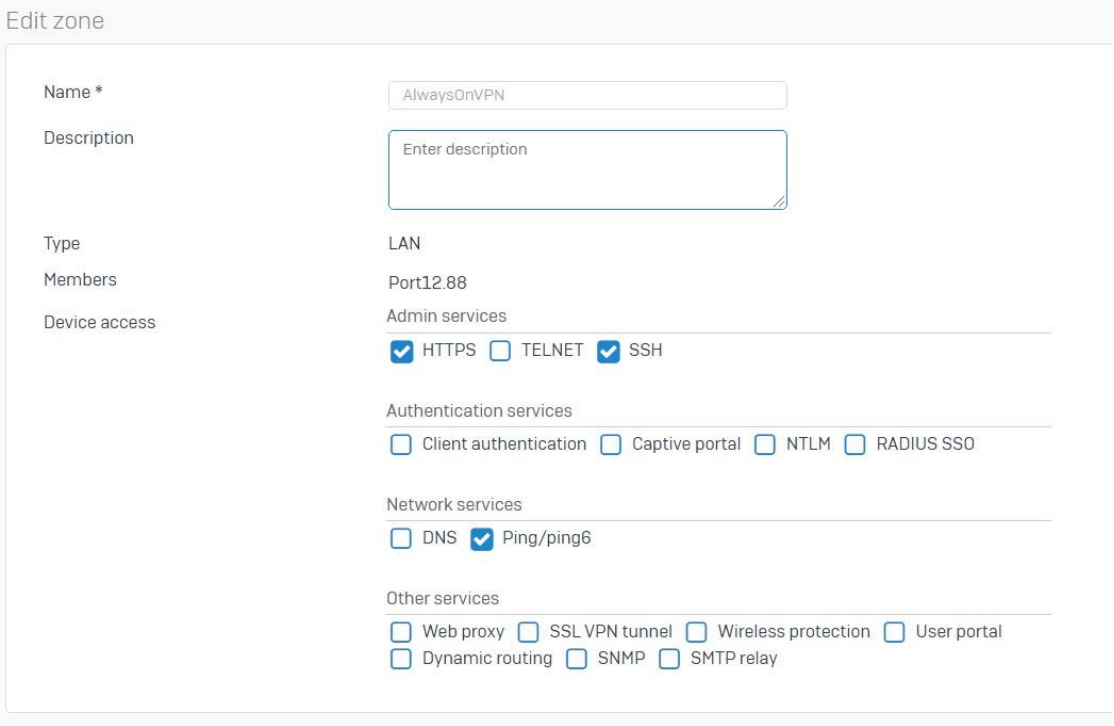
Kuvio 28. PEAP properties

Kun nämä määritykset oli saatu tehtyä, määritettiin käyttäjäryhmä, jonka käyttäjillä on oikeus käyttää VPN-yhteyttä. Tähän valittiin aiemmin luotu ryhmä **VPN Users**, jonka jäseneksi oli määritetty testikäyttäjä (ks. Taulukko 2). Muihin asetuksiin ei tässä vaiheessa tehty muutoksia, joten jatkettiin loppuun ja hyväksyttiin tehdyt määritykset.

5.3.3 Palomuurin ja kytkimien konfigurointi

Kuten luvussa 5.3.1 mainittiin, VPN-palvelin tarvitsee toimiakseen julkisen osoitteen, jotta se on saavutettavissa julkisesta verkosta. Liikenne ohjattiin palomuurilta testiympäristöön kahdella Yritys X:n kytkimellä, joihin lisättiin etäyhteyttä varten määritetty Vlan 88 ja hyväksyttiin sen liikenne valituista porteista.

Palomuurille luotiin uusi alue (zone) etäyhteysratkaisulle, joka määritettiin Vlan 88 mukaisesti porttiin 12.88 ja sen tyypiksi määritettiin lähiverkko (ks. Kuvio 29).

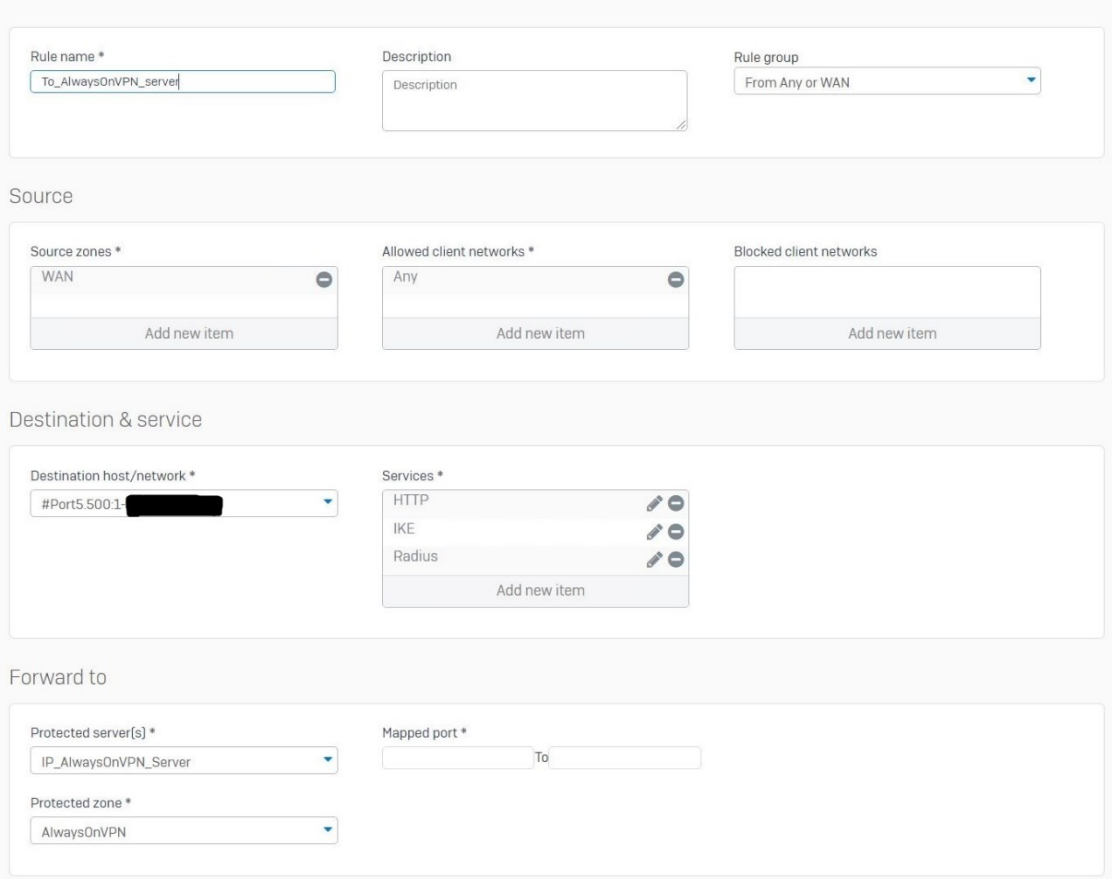


Kuvio 29. Always On VPN zone

Tämän jälkeen fyysinen rajapinta voidaan osoittaa kyseiseen alueeseen ja tehdä tarvittavat määritykset Vlanin osalta, joka kuuluu alueeseen (ks. Kuvio 30). Rajapinnan IP-osoitteeksi määritettiin 10.27.88.1.

Kuvio 30. Always On VPN Vlan määritykset

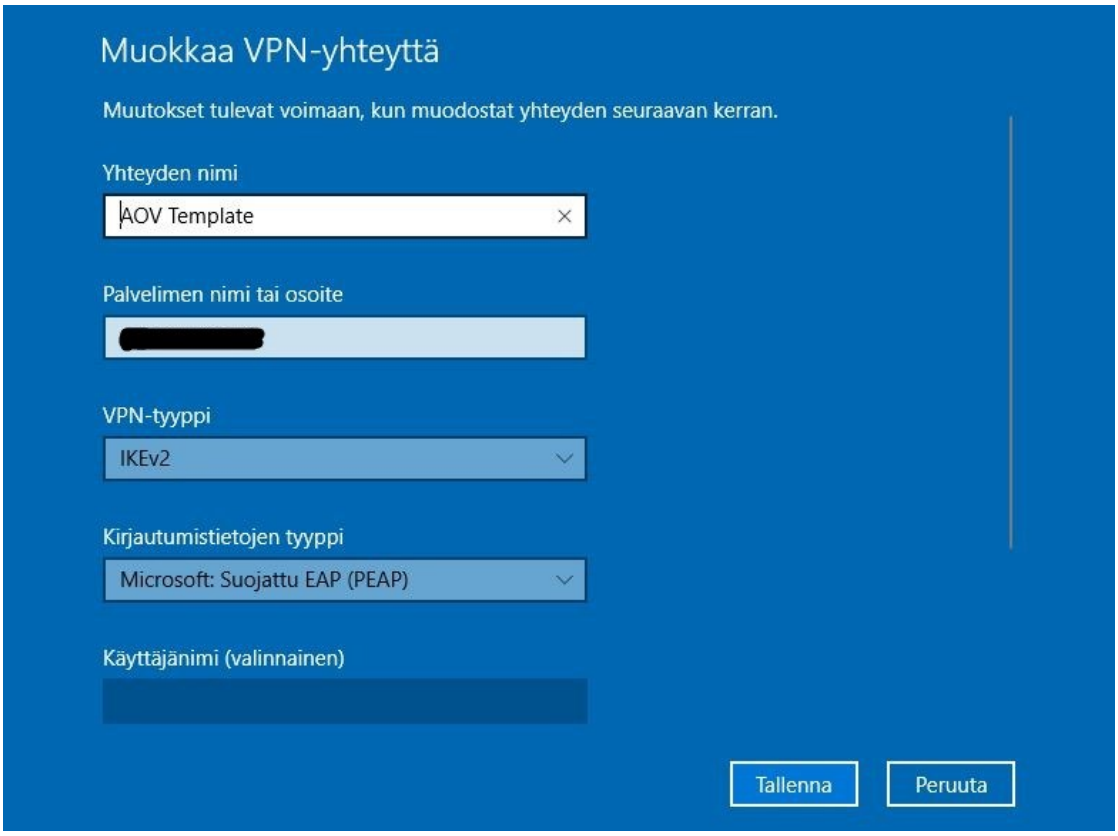
Tämän lisäksi palomuurille tehtiin ohjaussääntö (forward rule), jonka avulla määritettiin mitä liikennettä sallittiin julkiseen osoitteeseen (ks. Kuvio 31). Kuviosta on piilotettu julkinen osoite. Kohdeverkkoon sallittiin tärkeimpinä palveluina HTTP ja IKE. HTTP sallittiin testaustarkoituksia varten ja IKE, jotta varmistetaan IKE-yhteyksien toiminta. RADIUS-palvelua ei reunapalomuurille ole tarpeellista määrittää, vaan sitä käytettäisiin palomuurilla, joka sijaitsisi VPN-palvelimen takana.



Kuvio 31. Always On VPN forward rule

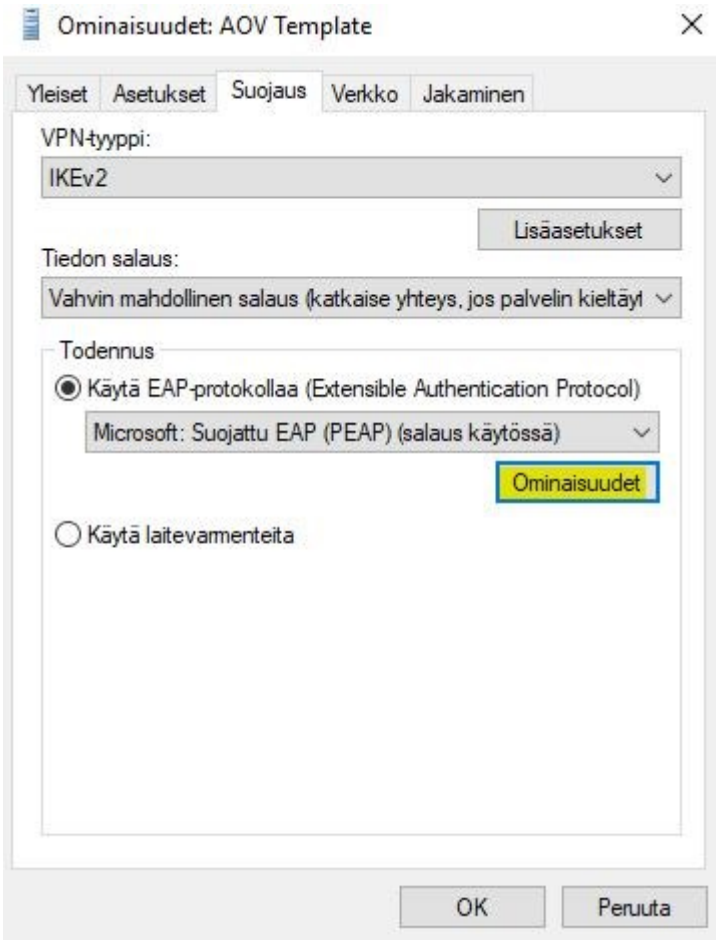
5.3.4 Testaus ja todennus

Kun konfigurointi oli saatu palvelimien osalta valmiiksi, aloitettiin etäyhteyden testaus, johon hyödynnettiin kannettavaa tietokonetta, joka oli liitetty toimialueeseen. Testaus toteutettiin aluksi manuaalisesti, sillä jotta automatisointiprofiileja voidaan hyödyntää, tulee varmistaa, että yhteys varmasti toimii. Kannettavalle tietokoneelle kirjauduttiin aluksi käyttäjällä, jolle oli määritetty oikeus etäyhteyden käyttöä varten (ks. Taulukko 2) ja määritettiin uusi VPN-yhteys manuaalisesti Windowsin asetuksista (ks. Kuvio 32). Yhteyden nimi päätettiin itse, osoitteeksi lisättiin julkinen osoite, joka on piilotettu kuvasta ja tyypiksi IKEv2. Tässä vaiheessa yhteysasetukset voitiin jo tallentaa, sillä niitä muokataan vielä lisää ohjauspaneelin verkkoyhteyksistä.



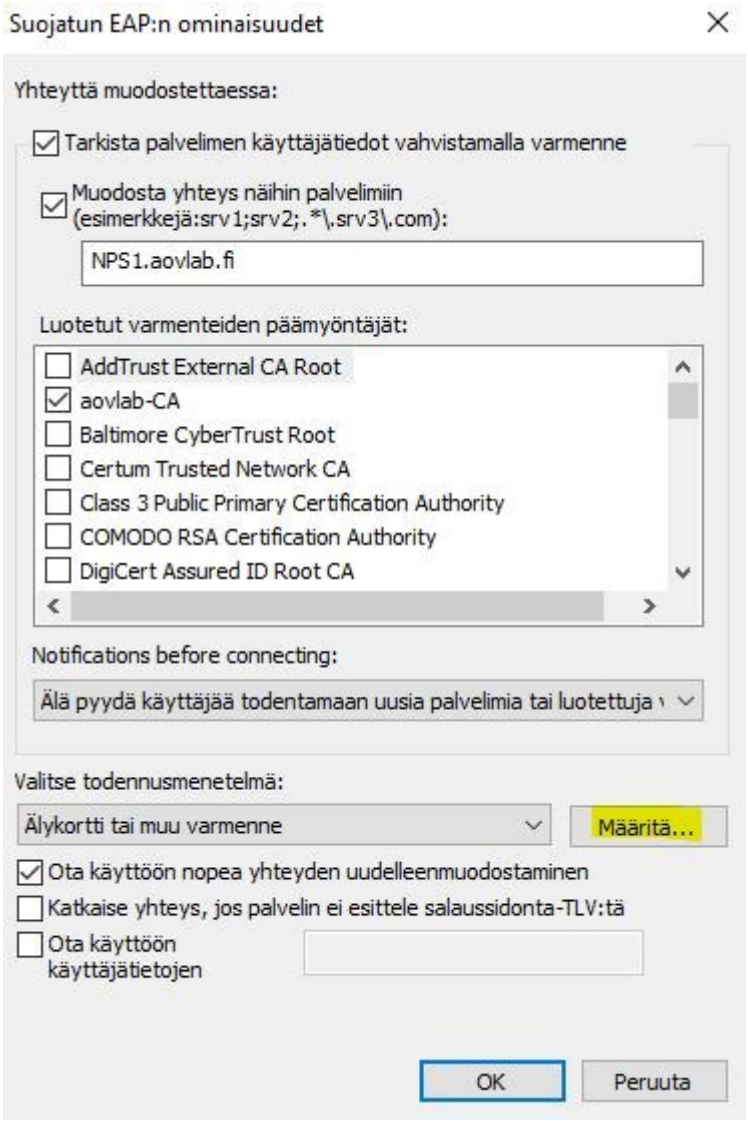
Kuvio 32. Uusi VPN-yhteys

Seuraavaksi tehtiin lisää määrityksiä etäyhteyden asetuksiin, jotka pystyttiin tekemään muuttamalla etäyhteyden sovitinasetuksia. Sovittimen asetuksissa siirryttiin aluksi **Suojaus** välilehdelle (ks. Kuvio 33), jossa vaihdettiin **Tiedon salaus** kohtaan **Vahvin mahdollinen salaus** ja todennusmenetelmäksi **Microsoft: Suojattu EAP (PEAP)**. Tämän jälkeen PEAP:n ominaisuuksiin piti tehdä vielä muutoksia, joita päästiin tekemään **Ominaisuudet** painikkeesta.



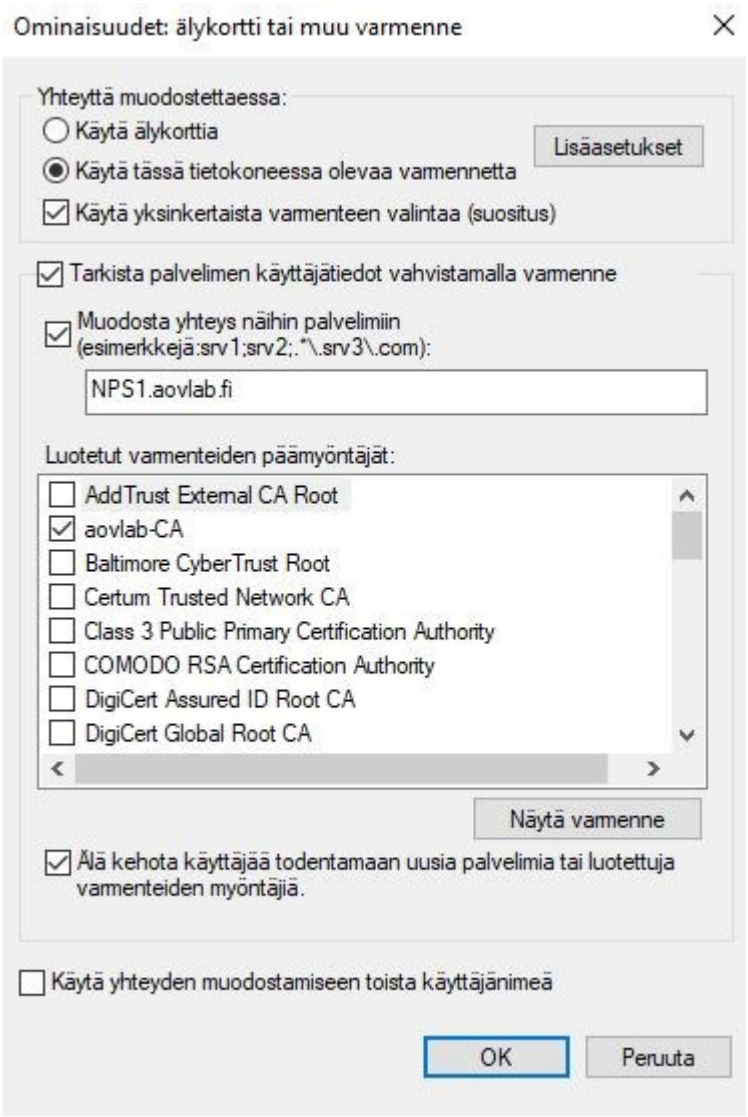
Kuvio 33. VPN-yhteyden sovitinasetukset

Ominaisuuksissa määritettiin aluksi yhteyden muodostaminen NPS-palvelimeen ja kyseisen palvelimen todennus varmenteen vahvistamisella. Palvelimen nimi, johon yhdistetään, tulisi olla sama kuin NPS-palvelimen todennusmenetelmien konfiguroin-tivaiheessa (ks. Kuvio 28). Luotettujen varmenteiden päämyöntäjiin valittiin oma CA nimi ja ilmoitukset ennen yhdistämistä otettiin pois käytöstä. Todennusmenetel-mäksi valittiin **Älykortti tai muu varmenne**, sillä varmenteita käytetään todennuk-sessa (ks. Kuvio 34). Lopuksi todennusmenetelmään täytyi tehdä vielä määrityksiä, jotka pystyttiin tekemään **Määritä** painikkeesta.



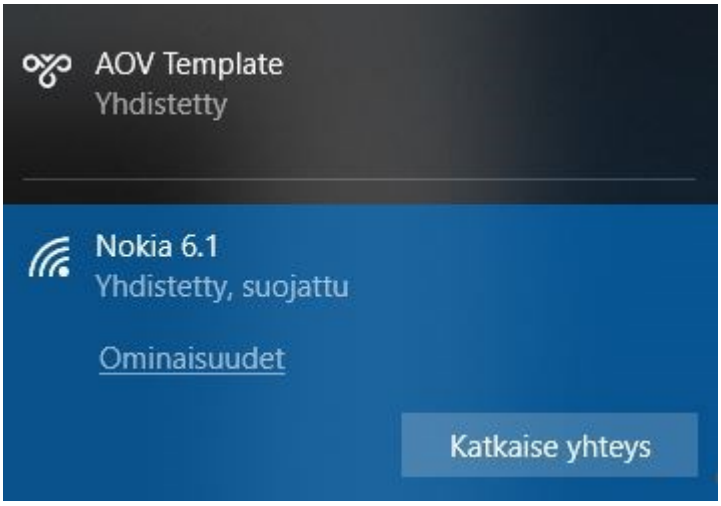
Kuvio 34. PEAP:n ominaisuudet

Todennusmenetelmän ominaisuuksissa tehtiin hyvin samanlaisia määrityksiä, kuin PEAP:n määrityksissä. Aluksi määritettiin käytettäväksi varmennetta, joka sijaitsee kyseisessä tietokoneessa ja tämän jälkeen tehtiin samat määritykset palvelimen varmenteen vahvistamiselle ja palvelimen nimelle, johon yhdistetään. Varmenteiden päämyöntäjäksi valittiin oma CA nimi ja lisättiin valinta, ettei käyttäjien tarvitse todentaa uusia palvelimia tai luotettuja varmenteiden myöntäjiä (ks. Kuvio 35). Lopuksi kaikki tehdyt määritykset hyväksyttiin.



Kuvio 35. Todennusmenetelmän ominaisuudet

Kun VPN-yhteysprofiili oli saatu määritettyä valmiiksi, suoritettiin lopullinen testaus, jossa kannettava tietokone irrotettiin testiympäristön kytkimestä ja yhdistettiin puhelimesta jaettuun yhteyspisteeseen. Tämän jälkeen yhdistettiin luotuun VPN-yhteysprofiiliin ja yhteys muodostui (ks. Kuvio 36).



Kuvio 36. Yhteysprofiilin testaus

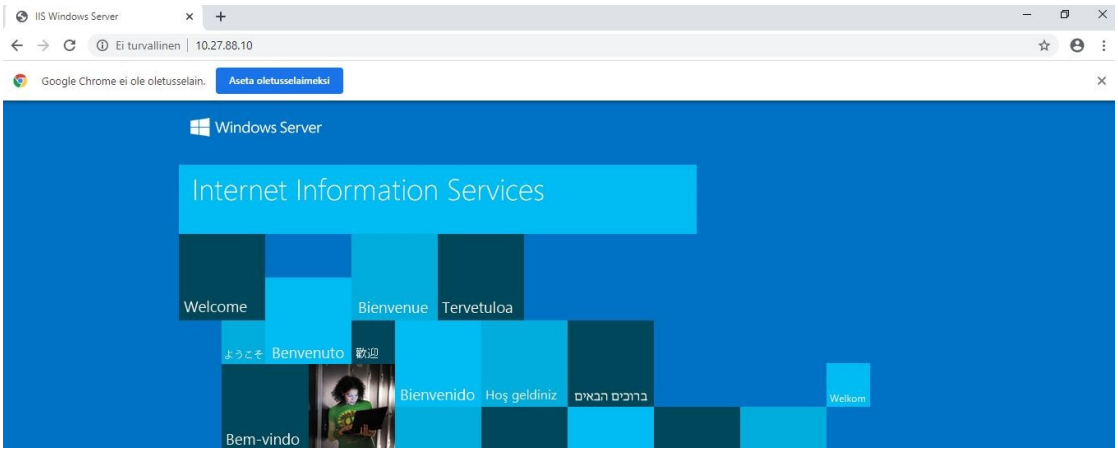
Kun yhteys oli muodostettu, tarkasteltiin saatuja osoitteita *ipconfig* -komennolla, joista huomattiin, että osoitteet ovat oikeasta osoiteavaruudesta, joka asetettiin käyttöön VPN-palvelimen konfiguroinnissa (ks. Kuvio 37).

```
PPP adapter AOV Template:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : AOV Template
   Physical Address. . . . . . . . . :
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.10.201(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.255
   Default Gateway . . . . . . . . . : 0.0.0.0
   DNS Servers . . . . . . . . . . . : 192.168.10.21
                                       8.8.8.8
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

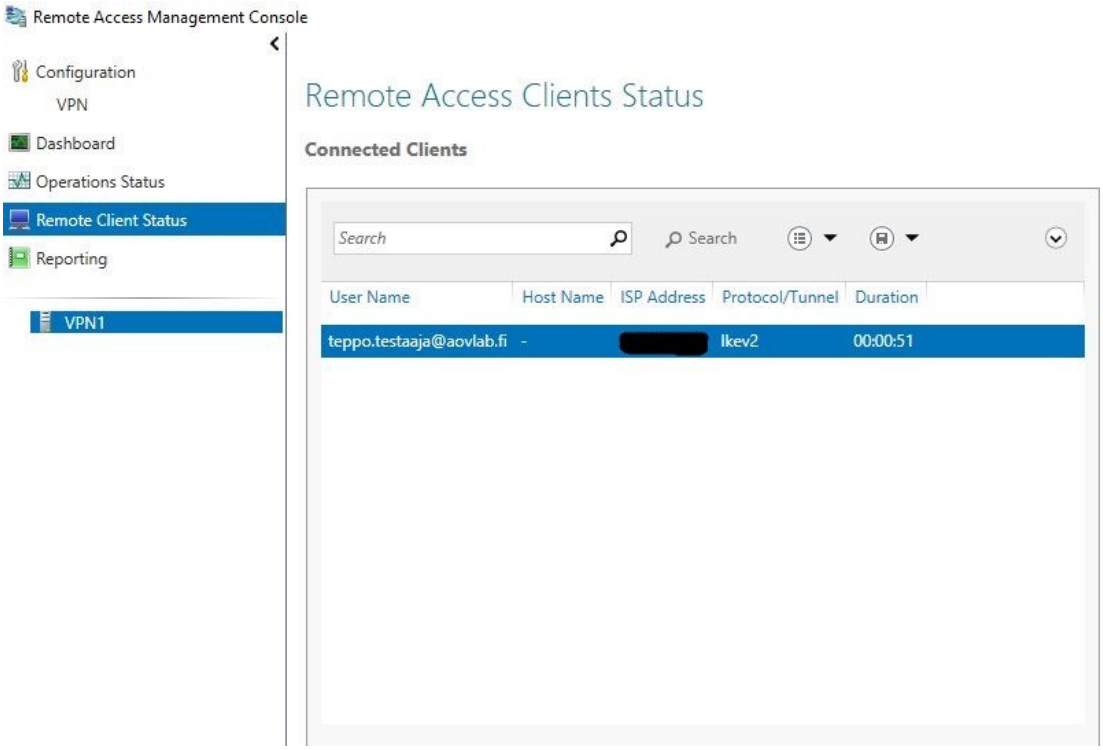
Kuvio 37. Yhteysprofiilin PPP-sovitin

Testausta varten VPN-palvelimelle otettiin myös käyttöön Internet Information Services (IIS), jonka avulla pystyttiin testaamaan yhteyttä sen tarjoamalle verkkosivulle, joka on tavoitettavissa ainoastaan sisäverkosta. Palvelun osoitteeksi määritettiin 10.27.88.10, eli VPN-palvelimen osoite. Kannettavalla tietokoneella syötettiin osoite selaimeen ja IIS-palvelun sivu avautui (ks. Kuvio 38). Tarkoituksena tällä testauksella oli todentaa, että kannettavalla tietokoneella oli mahdollista yhdistää sisäverkon resursseihin.



Kuvio 38. IIS-todennus

Näiden lisäksi haluttiin vielä varmistaa, että käytettävä VPN-protokolla on varmasti IKEv2 ja tämä tarkastettiin VPN-palvelimen etäyhteysasiakkaiden statuksesta (ks. Kuvio 39). Kuviosta on piilotettu puhelimen julkinen IP-osoite.



Kuvio 39. Remote Access Clients Status

5.3.5 VPN-profiilien automatisointi

Kun yhteyden testaus manuaalisesti oli toteutettu onnistuneesti, aloitettiin VPN-profiilien automatisointi. Automatisointi toteutettiin käyttäjälle ja siihen hyödynnettiin powershell skriptiä, joka luo jo olemassa olevasta etäyhteysprofiilista kaksi tiedostoa, joiden avulla automatisointi voidaan toteuttaa. Powershell skriptinä käytettiin Microsoftin verkkosivuilla olevaa malliskriptiä, johon vaihdettiin testiympäristön VPN-profiilin tiedot (ks. Liite 1). Muutoksia tehtiin vain ensimmäisille riveille (ks. Kuvio 40). **$TemplateName** kohtaan määritettiin olemassa olevan VPN-profiilin nimi, eli toisin sanoen manuaalisessa testissä käytetty VPN-profiilin nimi (ks. Kuvio 36). **$ProfileName** kohtaan pystyttiin määrittämään mikä tahansa nimi, joka tulee näkymään itse profiilissa. **$Servers** kohtaan määritettiin julkinen IP-osoite, jota ei kuvassa näytetä. **$DnsSuffix** kohtaan määritettiin DNS-pääte, jota käytetään profiilissa. **$DomainName** kohtaan määritettiin verkkotunnuksen jälkiliite, jota käytetään liitteenä DNS tarkkuuden kyselyyn. Kyseiseen kohtaan olisi ollut mahdollista sijoittaa toisena vaihtoehtona FQDN. **$DNSServers** kohtaan määritettiin profiilin käyttämät DNS-palvelimet. **$TrustedNetwork** kohtaan määritettiin luotettavan verkon nimi, jossa VPN ei yhdistä automaattisesti. (Step 6. Configure Windows 10 client Always On VPN connections 2018.)

```
$TemplateName = 'AOV Template'
$ProfileName = 'Aovlab AlwaysOn VPN'
$Servers = 'julkinen IP-osoite'
$DnsSuffix = 'aovlab.fi'
$DomainName = '.aovlab.fi'
$DNSServers = '192.168.10.21,8.8.8.8'
$TrustedNetwork = 'aovlab.fi'
```

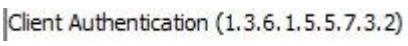
Kuvio 40. Malliskriptin määritykset

Kun tarvittavat määritykset oli saatu tehtyä, skripti ajettiin onnistuneesti ja kaksi tiedostoa ilmestyi työpöydälle. Tiedostot olivat VPN_Profile.ps1, eli powershell skripti, jonka avulla VPN-profiilia pystyttiin testaamaan manuaalisesti sekä VPN_Profile.xml, jota voitaisiin hyödyntää MDM-ratkaisuissa, kuten Microsoft Intune laitehallinnassa tai jos käytössä olisi SCCM.

Seuraavaksi VPN_Profile.ps1 suoritettiin järjestelmänvalvojana, jolloin uusi VPN-profiili saatiin luotua käyttäjälle. Automaatio testattiin yhdistämällä kannettava tietokone puhelimesta jaettuun verkkoon, jolloin VPN-profiili aktivoitui automaattisesti.

Luotua VPN-profiilia testattiin siis käyttäjätunnelina, eli automaatio otettiin käyttöön ainoastaan testikäyttäjälle. Kyseinen tapa ei ole optimaalisin vaihtoehto, sillä yhdistämistä ei pystytä tekemään ennen käyttäjän kirjautumista. Siksi tätä toteutusta käytettiin lähinnä testaamistarkoituksissa. Tuotantoympäristössä laitetunnelin käyttäminen olisi paras vaihtoehto.

Jos automaatio toteutettaisiin laitetunnelina, tarvittaisiin uusi sertifikaatti, joka on kohdistettu laitteelle ja tämän lisäksi laite täytyisi lisätä oikeaan käyttäjäryhmään, jotta NPS-palvelin sallii yhdistämisen. Sertifikaatin tulisi sisältää EKU-arvot asiakkaan todentamiseen (ks. Kuvio 41). Laitetunneleiden käyttöönotossa tulisi hyöyntää aiemmin luotua VPN_Profile.xml tiedostoa.



Kuvio 41. EKU-arvot asiakkaan todentamiseen

6 Tulokset ja yhteenveto

Opinnäytetyön tarkoituksena oli vertailla kahta etäyhteysratkaisua ja perehtyä uuteen ratkaisuun, sekä sen toimintaan. Tutkimuskysymyksiin liittyviä vastauksia on etsitty molemmista toteutuksista, sekä niihin liittyvistä teoriapohjaisista lähteistä. Tutkimuskysymyksissä on myös pohdittu asioita tuotantoympäristön näkökulmasta. Vertailussa tutkittiin molempien ratkaisujen palvelinympäristöjä, niiden käyttämiä palveluita ja kokonaisuuden muodostumista.

Mitä toimivaan Always On VPN -etäyhteysympäristöön tarvitaan?

Toimiva Always On VPN etäyhteysympäristö tarvitsee palvelinten osalta DC, CA, NPS, VPN palvelimet, jotka voivat olla virtuaalipalvelimia. Toteutus virtuaalipalvelimilla on todennäköisin ja myös luonnollisin tapa toteuttaa ratkaisu tänä päivänä. Virtuaalipalvelimia varten tarvitaan myös Hyper-V palvelin, johon muut virtuaalipalvelimet otetaan käyttöön. Tämän lisäksi tarvitaan yksi tai useampi palomuuri toteutustavan mukaan. Palomuurien avulla liikenne voidaan ohjata VPN-palvelimelle ja kahden palomuurin toteutuksessa, jossa VPN-palvelin sijaitsee palomuurien välissä, myös muille palvelimille. Tämän lisäksi tarvitaan yksi julkinen osoite, joka voi olla myös ulkoinen DNS-nimi. Palveluiden osalta tarvitaan toimiva AD-ympäristö, PKI ja DNS. Palvelinten käyttöjärjestelmien omana suosituksena on käyttää uusinta mahdollista vaihtoehtoa, eli tässä tapauksessa Windows Server 2019 käyttöjärjestelmää, mutta ratkaisu on mahdollista toteuttaa myös aikaisemmillakin käyttöjärjestelmillä, kuten esimerkiksi Windows Server 2016. Etäyhteyttä käyttävien työasemien käyttöjärjestelmässä on myös huomioitava, että Always On VPN on tuettu ainoastaan Windows 10 käyttöjärjestelmillä. Tuotantoympäristön toteutuksessa on myös huomioitava VPN-profiilien jakelu työasemille, jonka toteuttamiseen voidaan hyödyntää MDM-ratkaisuja, kuten Microsoft Intunea.

Kuinka Always On VPN -etäyhteysympäristö pystytetään?

Always On VPN ympäristön pystyttäminen riippuu paljon ympäristöstä, johon se ollaan ottamassa käyttöön, mutta yleisesti ottaen sen tarjoama yksinkertaisuus helpottaa huomattavasti toteutuksen suunnittelua ja käyttöönottoa. Useassa tuotantoympäristössä on jo valmiina monia tarvittavia asioita ratkaisun käyttöönottoon liittyen, eikä kaikkea tarvitse tehdä puhtaalta pöydältä, vaan asioita voidaan muokata/lisätä tilanteen mukaan. Alustava suunnitelma on kuitenkin tärkeä toteuttaa, sillä erityisesti VPN-profiilien jakaminen työasemille on toteutettu huomattavasti eri tavalla, kuin esimerkiksi Direct Access toteutuksissa. Ympäristön pystyttämisen suunnittelussa kannattaakin lähteä aluksi kartoittamaan jo olemassa olevia palvelimia ja niiden käyttöä osana ratkaisua. Oma mielipiteeni tuotantoympäristön toteutuksessa on jo olemassa olevien DC- ja CA-palvelimien hyödyntäminen ja niiden rinnalle uusien NPS- ja VPN-palvelimien pystyttäminen. Olemassa olevia VPN- ja NPS-palvelimia voidaan tietenkin hyödyntää muokkaamalla niiden konfiguraatioita, mutta tämä voi aiheuttaa ongelmia nykyisen VPN-tekniikan toimivuudessa ja tämä ei ole palveluiden toimivuuden näkökulmasta hyvä asia. Uudet palvelimet takaavatkin tämän vuoksi järjestelmänvalvojille vähemmän suunnittelua olemassa olevien palveluiden toimivuuden ylläpitämiseksi ja tämä helpottaa myös uuden ratkaisun testaamista. Uudet palvelimet voivat tietenkin lisätä joissakin toteutuksissa reitityssääntöjen lisäämistä ja palomuurien konfiguroimista.

Miten Always On VPN eroaa nykyisestä Direct Access -etäyhteysratkaisusta?

Vertailussa kahden hyvin samankaltaisen etäyhteysratkaisun välillä tutkittiin miten ympäristöt eroavat palvelinten, käytettävien protokollien ja VPN-profiilien jakamisen osalta. Palvelinten osalta eroja on VPN-palvelimessa, joka määritetään Direct Access toteutuksessa luonnollisesti Direct Access palvelimeksi ja Always On VPN toteutuksessa RRAS-palvelimeksi. Direct Access käyttää NLS-palvelimia määrittääkseen ovatko yhdistettävät koneet sisä- vai ulkoverkossa. Always On VPN ei tarvitse tähän erillistä palvelinta, vaan se hyödyntää yhdistettävän laitteen DNS-liitettä. Tunnelointiprotokollana Direct Access käyttää tässä tapauksessa IP-HTTPS tunnelia, jota käytetään IPv6-liikenteen tunneloimiseen IPv4-verkoissa. Always On VPN käyttää IKEv2 tunnelointiprotokollaa, johon ei tarvita IPv6-osoitteita. Yksi oleellisimmista eroista näiden kahden ratkaisun välillä onkin, että Direct Access käyttää IPv6-osoitteenvaihtoa,

kun taas Always On VPN tukee IPv4-osoitteita. VPN-profiilien jakaminen käyttäjien laitteilla tapahtuu Direct Access toteutuksessa GPO:n avulla, kun taas Always On VPN toteutuksissa on mahdollista hyödyntää MDM-ratkaisuja. Tuettujen käyttöjärjestelmien osalta Always On VPN tukee ainoastaan Windows 10 käyttöjärjestelmiä, kun taas Direct Access on mahdollista ottaa käyttöön myös Windows 7 käyttöjärjestelmillä. Always On VPN ratkaisu mahdollistaa myös paljon uusia ominaisuuksia, joilla esimerkiksi tietoturvaa voidaan parantaa. Esimerkkinä Azure MFA ja Windows Hello for Business. Käyttäjiä on molemmissa ratkaisuissa mahdollista monitoroida VPN-palvelimen kautta (ks. Kuvio 39), jota voidaan hyödyntää ongelmatilanteissa. Yleisellä tasolla ratkaisuja tarkastellessa voidaan todeta, että molemmat ovat hyvin samankaltaisia ja ne toimivat käyttäjän näkökulmasta lähes identtisesti. Järjestelmänvalvojan näkökulmasta Always On VPN vaikuttaa selkeämmältä ratkaisulta ja ympäristön pystyttäminen on myös todennäköisesti helpompi toteuttaa.

Yhteenveto

Molemmat ratkaisut ovat pääpiirteittäin hyvin samankaltaisia, joka on erittäin hyvä asia, sillä loppukäyttäjän käyttökokemus ei muutu. Kysymyksenä onkin tuoko Always On VPN lisäarvoa Direct Access -toteutuksiin niiden samankaltaisuuden vuoksi. Tähän kysymykseen oma mielipiteeni on, että Always On VPN tuo paljon uusia ominaisuuksia, joilla voidaan esimerkiksi parantaa tietoturvaa ja tämä tuo jo yksin painoarvoa ratkaisulle, sillä tietoturva on yksi tärkeimmistä asioista yrityksien infrastruktuureissa. Se että onko siirtyminen uuteen ratkaisuun välttämätöntä tehdä heti, ei mielestäni ole tarpeellista, mutta perehtyminen uuteen tekniikkaan on ainakin suositeltavaa aloittaa mahdollisimman pian, jotta kun siirtymävaihe tekniikasta toiseen alkaa, tarvittavat tiedot uudesta tekniikasta on hankittu etukäteen. Always On VPN on tulevaisuuden ratkaisu, joka tulee syrjäyttämään Direct Access ratkaisun, kun sen tuki päätetään ja tähän peilaten jokaisen yrityksen, joka haluaa säilyttää samat toiminnot, kuin Direct Access, kannattaa Always On VPN ratkaisuun perehtyminen aloittaa mahdollisimman pian.

Tutkittavista asioista voidaan yhteenvetona todeta, että asetettuihin tutkimuskysymyksiin pystyttiin vastaamaan suhteellisen kattavasti, sekä ottamaan myös kantaa asioihin omasta näkökulmasta. Tuloksena saatiin toteutettua testiympäristö Yritys

X:n käyttöön, sekä tietoa uudesta etäyhteysratkaisusta. Testiympäristöä ja hankittua tietoa voidaan hyödyntää tuotantoympäristön ratkaisun suunnittelussa ja käyttöönotossa.

7 Pohdinta

Opinnäytetyön päämääränä oli tutkia suhteellisen uutta tekniikkaa, perehtyä sen käyttöönottoon ja näin ollen muodostaa selkeä kuva etäyhteysratkaisun kokonaisuudesta. Jo suunnitteluvaiheessa etäyhteysratkaisu päätettiin toteuttaa testiympäristöön, joka oli hyvä ratkaisu, sillä työn edetessä vastaan tuli muutamia ongelmia, joiden selvittäminen oli riskitöntä testiympäristön takia. Erilaisten ongelmien selvittäminen muodostui välillä vaikeaksi, sillä tekniikasta ei työn toteuttamisen ajankohtana ollut monia lähteitä, joita olisi voinut hyödyntää ongelmanratkaisussa. Vaikka ongelmia esiintyikin, saatiin ne ratkaistua muutaman valvotun yön jälkeen.

Jatkossa testiympäristöllä voidaan toteuttaa erilaisia testauksia Always On VPN – etäyhteydelle, joista yhtenä esimerkkinä on automaattisen laitetunnelin muodostaminen, jota ei opinnäytetyössä käsitelty kuin teoreettisesti. Useita vaihtoehtoisia asioita ei käsitelty opinnäytetyössä, sillä aihe oli rajattava järkevästi. Tarkoituksena on opinnäytetyön lisäksi toteuttaa käyttöönottoon liittyvä ”step-by-step” ohje ja lisätä tähän myös opinnäytetyössä käsittelemättömät asiat sekä ongelmanratkaisuun liittyviä asioita.

Kokonaisuutena opinnäytetyön toteuttaminen oli mielenkiintoinen ja hyvin opettavainen kokemus, sillä aiempaa kokemusta VPN-tekniikoiden käyttöönotosta ei ollut. Tämän lisäksi uusien tekniikoiden tutkiminen, niiden käyttöönotto ja testaus ovat aina kiinnostaneet, joten työn toteuttaminen oli mielekästä. Aikataulun suunnittelussa huomasin puutteita, joihin tulee jatkossa kiinnittää enemmän huomiota. Tähän vaikutti tietenkin myös osittain opinnäytetyön tekemisen hetkellä vaikuttanut globaali pandemia, joka aiheutti erinäisiä muutoksia aikatauluissa ja lisäsi muuta kiirettä omissa työtehtävissä.

Lähteet

Always On VPN deployment for Windows Server and Windows 10. N.d. Artikkeli Microsoftin verkkosivulla. Viitattu 6.4.2020. https://docs.microsoft.com/en-us/windows-server/remote/remote-access/vpn/always-on-vpn/deploy/always-on-vpn-deploy.

Always On VPN enhancements. 2018. Artikkeli Microsoftin verkkosivulla. Viitattu 7.4.2020. https://docs.microsoft.com/en-us/windows-server/remote/remote-access/vpn/always-on-vpn/always-on-vpn-enhancements.

Always On VPN features and functionalities. 2018. Artikkeli Microsoftin verkkosivulla. Viitattu 6.4.2020. https://docs.microsoft.com/en-us/windows-server/remote/remote-access/vpn/vpn-map-da.

Always On VPN technology overview. 2018. Artikkeli Microsoftin verkkosivulla. Viitattu 6.4.2020. https://docs.microsoft.com/en-us/windows-server/remote/remote-access/vpn/always-on-vpn/always-on-vpn-technology-overview.

Conklin, A., Cothren, C., Davis, R., White, G. & William, D. 2018. Chapter 11 - Authentication and Remote Access. Principles of Computer Security: CompTIA Security+ and Beyond, Fifth Edition (Exam SY0-501). Viitattu 5.4.2020. https://janet.finna.fi/, Books24x7.

Deal, R. 2006. Chapter 4 - PPTP and L2TP. The Complete Cisco VPN Configuration Guide. Viitattu 5.4.2020. https://janet.finna.fi/, Books24x7.

Deploy Always On VPN. 2018. Ohje Microsoftin verkkosivulla. Viitattu 10.4.2020. https://docs.microsoft.com/en-us/windows-server/remote/remote-access/vpn/always-on-vpn/deploy/always-on-vpn-deploy-deployment.

DirectAccess. 2020. Artikkeli Microsoftin verkkosivulla. Viitattu 10.4.2020. https://docs.microsoft.com/fi-fi/windows-server/remote/remote-access/directaccess/directaccess.

End-to-end Access Example. 2012. Esimerkkitoteutus Microsoftin verkkosivulla. Viitattu 10.4.2020. https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/ee382326(v%3dws.10).

Frahim, J & Santos, O. 2010. IPSec Remote-Access VPNs. Cisco ASA: All-in-One Firewall, IPS, Anti-X, and VPN Adaptive Security Appliance: Identify, Mitigate, and Respond to Network Attacks, Second Edition. Viitattu 5.4.2020. https://janet.finna.fi/, Books24x7.

Hicks, R. M. 2015. DirectAccess Network Location Server Guidance. Artikkeli Richard M. Hicks Consulting, Inc. verkkosivulla. Viitattu 10.4.2020. https://directaccess.richardhicks.com/2015/02/09/directaccess-network-location-server-guidance/.

Hicks, R. M. 2016. DirectAccess vs. VPN. Artikkeli Richard M. Hicks Consulting, Inc. verkkosivulla. Viitattu 10.4.2020. https://directaccess.richard-hicks.com/2016/02/08/directaccess-vs-vpn/.

Hicks, R. M. 2019. Always On VPN IKEv2 Features and Limitations. Artikkeli Richard M. Hicks Consulting, Inc. verkkosivulla. Viitattu 5.4.2020. https://directaccess.richard-hicks.com/2019/04/15/always-on-vpn-ikev2-features-and-limitations/.

Hicks, R. M. N.d. DirectAccess is now Always On VPN. Artikkeli Richard M. Hicks Consulting, Inc. verkkosivulla. Viitattu 6.4.2020. https://directaccess.richardhicks.com/directaccess-is-now-always-on-vpn/.

Internet Key Exchange version 2 (IKEv2) Protocol. N.d. Artikkeli Vocalin verkkosivulla. Viitattu 5.4.2020. https://www.vocal.com/secure-communication/internet-key-exchange-v-2/.

Järvenpää, E. 2006. Laadullinen tutkimus. SoberIT jatko-opintoseminaari. Luentomateriaali cs.tut.fi verkkosivulla. Viitattu 8.4.2020. http://www.cs.tut.fi/~ihtesem/k2007/materiaali/luento4.pdf.

Nayak, U. & Rao, U. H. 2014. Chapter 12 - Virtual Private Networks. The InfoSec Handbook: An Introduction to Information Security. Viitattu 5.4.2020. https://janet.finna.fi/, Books24x7.

Pernaa, J. 2013. Kehittämistutkimus tutkimusmenetelmänä. Artikkeli tuhat.helsinki.fi verkkosivulla. Viitattu 8.4.2020. https://tuhat.helsinki.fi/ws/portalfiles/portal/127650174/2013_Pernaa_KT_tutkimusmenetelmana_KT_kirja.pdf.

Protected Extensible Authentication Protocol (PEAP). N.d. Artikkeli techopedian verkkosivulla. Viitattu 6.4.2020. https://www.techopedia.com/definition/4068/protected-extensible-authentication-protocol-peap.

Rouse, M. 2005. Extensible Authentication Protocol (EAP). Artikkeli TechTargetin verkkosivulla. Viitattu 6.4.2020. https://searchsecurity.techtarget.com/definition/Extensible-Authentication-Protocol-EAP.

Step 1 Configure Advanced DirectAccess Infrastructure. 2020. Artikkeli Microsoftin verkkosivulla. Viitattu 10.4.2020. https://docs.microsoft.com/fi-fi/windows-server/remote/remote-access/directaccess/single-server-advanced/da-adv-configure-s1-infrastructure.

Step 1 Plan the Advanced DirectAccess Infrastructure. 2020. Artikkeli Microsoftin verkkosivulla. Viitattu 10.4.2020. https://docs.microsoft.com/fi-fi/windows-server/remote/remote-access/directaccess/single-server-advanced/da-adv-plan-s1-infrastructure#11-plan-network-topology-and-settings.

Step 6. Configure Windows 10 client Always On VPN connections. 2018. Artikkeli Microsoftin verkkosivulla. Viitattu 15.4.2020. https://docs.microsoft.com/en-us/windows-server/remote/remote-access/vpn/always-on-vpn/deploy/vpn-deploy-client-vpn-connections.

Stewart, J. M. 2014a. Chapter 3 - VPN Fundamentals. Network Security, Firewalls and VPNs, Second Edition. Viitattu 4.4.2020. https://janet.finna.fi/, Books24x7.

Stewart, J. M. 2014b. What Are the Limitations of a VPN?. Network Security, Firewalls and VPNs, Second Edition. Viitattu 4.4.2020. https://janet.finna.fi/, Books24x7.

VPN authentication options. 2017. Artikkeli Microsoftin verkkosivulla. Viitattu 5.4.2020. https://docs.microsoft.com/en-us/windows/security/identity-protection/vpn/vpn-authentication.

Liitteet

Liite 1. Microsoftin malliskripti

Malliskripti on saatavilla Microsoftin verkkosivulta ja sitä voidaan hyödyntää automaattisten VPN-profiilien luomisessa. VPN-profiilit luodaan muuttamalla ylimpiä arvoja oman ympäristön määritysten mukaisesti (ks. 5.3.5).

```
$TemplateName = 'Template'
 $ProfileName = 'Contoso AlwaysOn VPN'
 $Servers = 'vpn.contoso.com'
 $DnsSuffix = 'corp.contoso.com'
 $DomainName = '.corp.contoso.com'
 $DNSServers = '10.10.0.2,10.10.0.3'
 $TrustedNetwork = 'corp.contoso.com'


 $Connection = Get-VpnConnection -Name $TemplateName
 if(!$Connection)
 {
 $Message = "Unable to get $TemplateName connection profile: $_"
 Write-Host "$Message"
 exit
 }
 $EAPSettings= $Connection.EapConfigXmlStream.InnerXml

 $ProfileXML = @("
 <VPNProfile>
   <DnsSuffix>$DnsSuffix</DnsSuffix>
   <NativeProfile>
 <Servers>$Servers</Servers>
 <NativeProtocolType>IKEv2</NativeProtocolType>
 <Authentication>
   <UserMethod>Eap</UserMethod>
   <Eap>
    <Configuration>
     $EAPSettings
    </Configuration>
   </Eap>
 </Authentication>
 <RoutingPolicyType>SplitTunnel</RoutingPolicyType>
   </NativeProfile>
 <AlwaysOn>true</AlwaysOn>
 <RememberCredentials>true</RememberCredentials>
 <TrustedNetworkDetection>$TrustedNetwork</TrustedNetworkDetection>
   <DomainNameInformation>
 <DomainName>$DomainName</DomainName>
 <DnsServers>$DNSServers</DnsServers>
 </DomainNameInformation>
 </VPNProfile>
 ")
```

```
 $ProfileXML | Out-File -FilePath ($env:USERPROFILE + '\desk-
top\VPN_Profile.xml')

  $Script = @("
   `$ProfileName = '$ProfileName'
   `$ProfileNameEscaped = `$ProfileName -replace ' ', '%20'

   `$ProfileXML = '$ProfileXML'

   `$ProfileXML = `$ProfileXML -replace '<', '&lt;'
   `$ProfileXML = `$ProfileXML -replace '>', '&gt;'
   `$ProfileXML = `$ProfileXML -replace '`"', '&quot;'

   `$nodeCSPURI = `"./Vendor/MSFT/VPNv2`"
   `$namespaceName = `"root\cimv2\mdm\dmmap`"
   `$className = `"MDM_VPNv2_01`"

   try
   {
   `$username = Gwmi -Class Win32_ComputerSystem | select username
   `$objuser = New-Object System.Security.Principal.NTAc-
count(`$username.username)
   `$sid = `$objuser.Translate([System.Security.Principal.SecurityIden-
tifier])
   `$SidValue = `$sid.Value
   `$Message = `"User SID is `$SidValue.`"
   Write-Host `"`$Message`"
   }
   catch [Exception]
   {
   `$Message = `"Unable to get user SID. User may be logged on over Re-
mote Desktop: `$_`"
   Write-Host `"`$Message`"
   exit
   }

   `$session = New-CimSession
   `$options = New-Object Microsoft.Management.Infrastructure.Op-
tions.CimOperationOptions
   `$options.SetCustomOption(`"PolicyPlatformContext_PrincipalCon-
text_Type`", `"PolicyPlatform_UserContext`", `$false)
   `$options.SetCustomOption(`"PolicyPlatformContext_PrincipalCon-
text_Id`", `"`$SidValue`", `$false)

   try
   {
  `$deleteInstances = `$session.EnumerateInstances(`$namespaceName,
`$className, `$options)
  foreach (`$deleteInstance in `$deleteInstances)
  {
      `$InstanceId = `$deleteInstance.InstanceID
      if (`"`$InstanceId`" -eq `"`$ProfileNameEscaped`")
      {
          `$session.DeleteInstance(`$namespaceName, `$deleteInstance,
`$options)
          `$Message = `"Removed `$ProfileName profile `$InstanceId`"
          Write-Host `"`$Message`"
      } else {
```

```
          `$Message = `"Ignoring existing VPN profile `$InstanceId`"
          Write-Host `"`$Message`"
      }
  }
   }
   catch [Exception]
   {
  `$Message = `"Unable to remove existing outdated instance(s) of `$Pro-
fileName profile: `$_`"
  Write-Host `"`$Message`"
  exit
   }

   try
   {
  `$newInstance = New-Object Microsoft.Management.Infrastructure.CimIn-
stance `$className, `$namespaceName
  `$property = [Microsoft.Management.Infrastructure.CimProperty]::Cre-
ate(`"ParentID`", `"`$nodeCSPURI`", `"String`", `"Key`")
  `$newInstance.CimInstanceProperties.Add(`$property)
  `$property = [Microsoft.Management.Infrastructure.CimProperty]::Cre-
ate(`"InstanceID`", `"`$ProfileNameEscaped`", `"String`",      `"Key`")
  `$newInstance.CimInstanceProperties.Add(`$property)
  `$property = [Microsoft.Management.Infrastructure.CimProperty]::Cre-
ate(`"ProfileXML`", `"`$ProfileXML`", `"String`", `"Property`")
  `$newInstance.CimInstanceProperties.Add(`$property)
  `$session.CreateInstance(`$namespaceName, `$newInstance, `$options)
  `$Message = `"Created `$ProfileName profile.`"

  Write-Host `"`$Message`"
   }
   catch [Exception]
   {
  `$Message = `"Unable to create `$ProfileName profile: `$_`"
  Write-Host `"`$Message`"
  exit
   }

   `$Message = `"Script Complete`"
   Write-Host `"`$Message`"
   ")

   $Script | Out-File -FilePath ($env:USERPROFILE + '\desk-
top\VPN_Profile.ps1')

 $Message = "Successfully created VPN_Profile.xml and VPN_Profile.ps1 on
the desktop."
 Write-Host "$Message"
```